UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
MIDLAND-ODESSA DIVISION

Skysong Innovations, LLC,	)	
	)	
Plaintiff,	)	
	)	
v.	)	C.A. No. 7:25-cv-00040
	)	
CrowdStrike, Inc. and CrowdStrike Holdings, Inc.,	)	JURY TRIAL DEMANDED
	)	
	)	
Defendants.	)	

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Skysong Innovations, LLC ("Skysong") alleges against Defendants CrowdStrike, Inc. and CrowdStrike Holdings, Inc. (collectively "CrowdStrike" or "Defendants") the following:

NATURE OF THE CASE

1. This is a civil action for infringement of U.S. Patent No. 10,313,385 (the "'385 Patent"), U.S. Patent No. 11,275,900 (the "'900 Patent"), U.S. Patent No. 11,775,831 (the "'831 Patent"), and U.S. Patent No. 11,892,897 (the "'897 Patent" and collectively, the "Asserted Patents") arising under the Patent Laws of the United States, 35 U.S.C. §§ 271 *et seq*.

THE PARTIES

2. Plaintiff Skysong is a private nonprofit and the exclusive intellectual property management and technology transfer organization for Arizona State University ("ASU"). Skysong works with ASU faculty, researchers, and technology industry partners to translate ASU innovations into broad societal impact. Skysong's goal is the rapid and wide dissemination of intellectual property and inventions created by ASU to the marketplace.[1]

[1] *See* https://skysonginnovations.com/; https://skysonginnovations.com/about/.

3. ASU's charter, which is literally carved in stone on its Tempe campus, reads: "ASU is a comprehensive public research university, measured not by whom it excludes, but by whom it includes and how they succeed; advancing research and discovery of public value; and assuming fundamental responsibility for the economic, social, cultural and overall health of the communities it serves."[2] Founded in 1885 as Territorial Normal School by the 13th Arizona Territorial Legislature, ASU is the State of Arizona's largest university, with its largest campus located in Tempe, Arizona. ASU offers more than 400 academic undergraduate programs and majors led by expert faculty in highly ranked colleges and schools. ASU has over 183,000 enrolled students, of which more than 18,000 were veteran or military-affiliated students during fall 2024.[3] For example, U.S. News & World Report rates 84 ASU degree programs in the top 25 in the country, including 38 programs ranked in the nation's top 10.[4] A member of the Association of American Universities (comprising the country's leading research universities), ASU has over 400 faculty members elected to the National Academies of Science, with five of its faculty receiving the Nobel Prize. ASU has held the No. 1 ranking for innovation ten years in a row and is ranked in the top 10 worldwide among universities granted U.S. patents according to the National Academy of

[2] https://www.asu.edu/about/charter-mission.

[3] https://www.asu.edu/about/facts-and-figures.

[4] https://www.asu.edu/about/facts-and-figures.

Inventors.[5] In addition, ASU is ranked No. 2 in the country for employability among public universities; it is one of Arizona's largest employers with more than 18,500 employees.[6]

4. Each of the Asserted Patents is assigned to Skysong. Skysong is the exclusive owner of all rights, title, and interest in and to the Asserted Patents, and has the right to bring this suit to recover damages for any current or past infringement of the Asserted Patents.

5. On information and belief, Defendant CrowdStrike Holdings, Inc. is a Delaware corporation with its headquarters and principal place of business in this District.[7] Defendant CrowdStrike Holdings, Inc. is the parent of and directly and wholly owns Defendant CrowdStrike, Inc.

6. On information and belief, Defendant CrowdStrike, Inc. is a Delaware corporation with its headquarters and principal place of business in this District. Defendant CrowdStrike, Inc. is registered with the Secretary of State to conduct business in Texas.

7. Defendants provide cybersecurity software and systems that, without authorization, implement patented technologies invented by ASU. Defendants' infringing security software and services include, but are not limited to, the Falcon Platform, including certain related modules, features, and functionalities such as Falcon Exposure Management and Falcon Adversary

[5] https://news.asu.edu/20240923-university-news-asu-no-1-innovation-10-years-us-news-world-report-ranking#:~:text=University%20news-,A%20decade%20strong%3A%20ASU%20takes%20top%20spot%20in%20innovation,10th%20year%20in%20a%20row&text=For%20the%2010th%20year%20in,rankings%20earned%20by%20the%20university; https://academyofinventors.org/wp-content/uploads/2024/02/2023-Top-100-Worldwide.pdf; https://news.asu.edu/20240219-university-news-asu-ranked-no-9-worldwide-us-patents-2023.

[6] https://cfo.asu.edu/working-at-asu#:~:text=ASU%20is%20one%20of%20Arizona's,which%20starts%20with%20its%20employees.

[7] *See* https://www.crowdstrike.com/en-us/blog/crowdstrike-changes-principal-executive-office-to-austin-texas/.

Intelligence, as well as prior versions and functionalities that are the same or essentially same as that described herein (collectively, “Falcon Platform” or the “Accused Products”).

JURISDICTION AND VENUE

8. This is an action for patent infringement arising under the Patent Laws of the United States, including 35 U.S.C. §§ 271 *et seq*. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

9. This Court has personal jurisdiction over Defendants because they regularly conduct business in the State of Texas and in this District. This business includes operating systems, using software, and/or providing services and/or engaging in activities in Texas and in this District that infringe one or more claims of the Asserted Patents in this forum, as well as inducing and contributing to the direct infringement of others through acts in this District.

10. Defendants have also, directly and through their extensive network of partnerships, including with local IT service providers, purposefully and voluntarily placed products and/or provided services that practice the methods claimed in the Asserted Patents into the stream of commerce with the intention and expectation that they will be purchased and used by customers in this District, as detailed below.[8]

11. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b) and (c), and 28 U.S.C. § 1400(b).

12. On information and belief, Defendants have regular and systematic contacts within this District and have committed acts of infringement within this District. For example, CrowdStrike Holdings, Inc.’s “principal executive offices occupy approximately 47,618 square feet in Austin, Texas under a lease that expires in 2030.” Additionally, Defendant CrowdStrike

[8] *See* https://www.crowdstrike.com/en-us/partners/channel-partners/.

Holdings, Inc. wholly-owns Defendant CrowdStrike, Inc., and controls Defendant CrowdStrike, Inc.'s contacts and activities, including contacts with and acts of infringement in this District.[9]

13. Defendant CrowdStrike, Inc. is a registered business in Texas and has regular and established places of business in this District.[10] On information and belief, Defendant CrowdStrike, Inc. has hundreds of employees in this District, including positions in engineering, sales, marketing, and finance, and some of whom may have relevant information, including information concerning the products and services Defendants provide and how those products operate.

14. Defendants have committed acts of infringement within this District. For example, on information and belief, Defendants use the Accused Products in this District in manners that practice the Asserted Patents, including by testing the Accused Products and by using the Accused Products at their offices in this District.

15. On information and belief, Defendants make, use, advertise, offer for sale, and/or sell endpoint security software (including the Accused Products) and provide security services that practice the Asserted Patents in the State of Texas and in this District directly and/or through their partnerships with businesses in the State of Texas and in this District.

16. On information and belief, Defendants sell, offer for sale, advertise, make, install, and/or otherwise provide endpoint security software and security services, including the Accused Products, the use of which infringe the Asserted Patents in this District and the State of Texas. Defendants perform these acts directly and/or through their partnerships with other entities.

[9] *See* https://ir.crowdstrike.com/static-files/29e71f45-3c39-4c2c-9159-5e7bb9f3315b ("CrowdStrike 2024 Annual Report Form 10-K") at 57, 71.

[10] *See, e.g.,* https://www.tdlr.texas.gov/TABS/Search/Print/TABS2021010277.

17. On information and belief, Defendants also use a network of partners, which comprise re-sellers, managed service providers and cybersecurity experts to provide the Accused Products and implementation of services for the Accused Products to their customers in this District. Each of these partners sells, offers for sale, and/or installs the Accused Products.

18. Defendants engage in activities that infringe the Asserted Patents (directly or indirectly) within this District. For example, Defendants' operation and use of the Accused Products within this District infringe (directly or indirectly) the Asserted Patents.

19. Defendants also infringe (directly or indirectly) the Asserted Patents by providing services in connection with the Accused Products including installing, maintaining, supporting, operating, providing instructions, and/or advertising the Accused Products within this District. End-users and partner customers infringe the Asserted Patents by installing and operating the Accused Products, which perform the claimed methods in the Asserted Patents within this District.

20. Defendants encourage and induce their customers of the Accused Products to perform the methods claimed in the Asserted Patents. For example, Defendants make their security services available on their website, widely advertise those services, provide applications that allow partners and users to access those services, provide instructions for installing, and maintaining those products, and provide technical support to users.[11]

21. Defendants further encourage and induce their customers to use the Accused Products by providing directions for and encouraging the "CrowdStrike Falcon agent" to be installed on individual endpoint computers, which offers evaluation, installation, configuration, customization, and development of the Falcon Platform.[12]

[11] *See* https://www.crowdstrike.com/en-us/contact-us/.

[12] *See* https://www.crowdstrike.com/tech-hub/endpoint-security/install-falcon-sensor-for-windows/.

PLAINTIFF'S PATENTED INNOVATIONS

22. The '385 Patent, titled "Systems and methods for data driven game theoretic cyber threat mitigation," was filed on November 28, 2016, and duly and legally issued by the USPTO on June 4, 2019. The '385 Patent claims priority to U.S. Provisional Application No. 62/261,200, which was filed on November 30, 2015. A true and correct copy of the '385 Patent is attached hereto as Exhibit 1.

23. The named inventors of the '385 Patent are Paulo Shakarian, John Robertson, Jana Shakarian, Vivin Paliath, and Amanda Thart.

24. The '385 Patent "relates to a security game frame-work, and in particular to a data-driven security game framework that models an attacker based on exploit market data actively mined from the 'darknet' or other overlay communication networks to develop strategies for the defender." (Exhibit 1, '385 Patent, 1:15-20.) At the time of the filing of the '385 Patent, "there d[id] not appear to be a game theoretic approach to host-based defense where the activities of the attacker are informed from an 'un-conventional' source (information not directly related to the defender's system) specifically information from darknet markets in this case." (*Id.* at 2:26-31.) To address these shortcomings, the '385 Patent "introduce[d] a rigorous and thoroughly analyzed framework for addressing penetration testing that is fed with real - world exploit market data, mined from the darknet." (*Id.* at 3:4-7.) In one embodiment, the '385 Patent employs a new security game frame-work "designed to model an attacker with access to exploit markets and a defender of information technology infrastructure; theoretical analysis of the framework leading to the development of algorithms to find near - optimal strategies for both players; and an implementation of the system and the results of a thorough suite of experiments on real-world data." (*Id.* at 3:8-15.)

25. Each claim in the ’385 Patent recites an independent invention. Neither claim 8, nor any other individual claim is representative of all claims in the ’385 Patent.

26. The ’385 Patent is valid and enforceable and enjoys a statutory presumption of validity pursuant to 35 U.S.C. § 282.

27. The ’900 Patent, titled “Systems and methods for automatically assigning one or more labels to discussion topics shown in online forums on the dark web,” was filed on May 7, 2019, and duly and legally issued by the USPTO on March 15, 2022. The ’900 Patent claims priority to U.S. Provisional Application No. 62/668,878, which was filed on May 9, 2018. A true and correct copy of the ’900 Patent is attached hereto as Exhibit 2.

28. The named inventors of the ’900 Patent are Revanth Patil, Paulo Shakarian, Ashkan Aleali, and Ericsson Marin.

29. The ’900 Patent covers “systems and methods for automatically assigning one or more labels or tags related to various discussion forum topics on the dark web or deep web” (Exhibit 2, ’900 Patent, 1:17-20). Malicious users of the internet seek “online platforms for illegal activities such as credit card fraud, identity theft, leaks of sensitive information and sharing hacking information” (*Id.* at 1:25-27). The dark web and deep web have “emerged in the last decade and contributed to the achievement of those criminal tasks” (*Id.* at 1:27-30). The ’900 Patent addresses the issue of the lack of efficient labelling and classification of information found on the “deep web that is not indexed by web search engines” (*Id.* at 1:63-64), as “[c]urrent technologies use learning models and techniques that do not address the issues of labeled data scarcity, nor do they address imbalanced data classes in the training set. Training sets are labeled by hand, which is a time-consuming and typically un-scalable process.” (*Id.* at 2:10-15). To address these shortcomings, the ’900 Patent claims techniques “includ[ing] an inventive computer-

implemented system […] that involves automatically assigning one or more labels (tags), in a hierarchical structure, to discussion topics seen" in deep-web forums (*Id*. at 3:10-14).

30. Each claim in the '900 Patent recites an independent invention. Neither claim 12, nor any other individual claim is representative of all claims in the '900 Patent.

31. The '900 Patent is valid and enforceable and enjoys a statutory presumption of validity pursuant to 35 U.S.C. § 282.

32. The '831 Patent, titled "Cascaded computing for convolutional neural networks," was filed on January 13, 2023, and duly and legally issued by the USPTO on October 3, 2023. The '831 Patent is a continuation of U.S. Patent Application No. 16/335,775 filed on March 22, 2019, which is a U.S. National Stage Application under 35 USC § 371 and claims the benefit of International Patent Application No. PCT/US2017/052736 filed on September 21, 2017, which claims priority to U.S. Provisional Patent Application No. 62/399,753 filed on September 26, 2016. A true and correct copy of the '831 Patent is attached hereto as Exhibit 3.

33. The named inventors of the '831 Patent are Jae-sun Seo and Minkyu Kim.

34. The '831 Patent is directed to techniques for "for efficiently reducing the amount of total computation in CNNs without affecting the output result or classification accuracy." (Exhibit 3, '831 Patent, 1:33-36). "Convolutional Neural Networks (CNNs) have gained popularity in many computer vision applications (image, video, speech, etc.), because of their ability to train and classify with high accuracy. Due to multiple layers of convolution and pooling operations that are compute-/memory-intensive, it is difficult to perform real-time classification with low power consumption on today's computing systems." (*Id*. at 1:22-29). To address these shortcomings, the '831 Patent claims innovative techniques that "can be embodied in methods that include actions of: in one or more layers of a convolutional neural network (CNN), performing a first iteration that

includes computing a value based on a first set of most significant bits (MSBs) for each of a plurality of data sets; examining a first set of values computed for the plurality of data sets in the first iteration to determine whether a maximum value is present among the first set of values; responsive to identifying the maximum value, performing a full precision computation of the value for a data set, of the plurality of data sets, that exhibited the maximum value; and propagating the full precision computation of the value to a subsequent layer of the CNN." (*Id*. at 1:37-50).

35. Each claim in the '831 Patent recites an independent invention. Neither claim 1, nor any other individual claim is representative of all claims in the '831 Patent.

36. The '831 Patent is valid and enforceable and enjoys a statutory presumption of validity pursuant to 35 U.S.C. § 282.

37. The '897 Patent, titled "Systems and methods for predicting which software vulnerabilities will be exploited by malicious hackers to prioritize for patching," was filed on October 26, 2018, and duly and legally issued by the USPTO on February 6, 2024. The '897 Patent claims priority to U.S. Provisional Application No. 62/581,123, which was filed on November 3, 2017. A true and correct copy of the '897 Patent is attached hereto as Exhibit 4.

38. The named inventors of the '897 Patent are Paulo Shakarian, Mohammed Almukaynizi, Jana Shakarian, Eric Nunes, Krishna Dharaiya, Manoj Balasubramaniam Senguttuvan, and Alexander Grimm.

39. The '897 Patent "relates to assessing the likelihood of exploitation of software vulnerabilities, and in particular to systems and methods for predicting which software vulnerabilities will be exploited by malicious hackers and hence prioritized by patching." (Exhibit 4, '897 Patent, 1:24-28). Prior to the '897 Patent, "current methods for prioritizing patching vulnerabilities appear to fall short." (*Id*. at 1:48-49). For example, prior-art methods: over-reported

"vulnerabilities as severe and will be exploited to be on the side of caution"; were "not an effective predictor of vulnerabilities being exploited"; and "were limited to single sites that provided a relatively small number of predictions" (*Id*. at 1:45-2:7). To overcome such issues, the inventions in the '897 Patent marshals "machine learning models described herein in predicting exploits in the wild" (*Id*. at 3:55-56) drawing upon "a variety of data sources or data feeds" (*Id*. at 3:27-29) to analyze exploited vulnerabilities. For instance, it further "leverages machine learning techniques on features derived from the social network of users participating in darkweb/deepweb (DW) forums, as well as features derived from the National Vulnerability Database." (*Id*. at 4:20-23).

40. Each claim in the '897 Patent recites an independent invention. Neither claim 1, nor any other individual claim is representative of all claims in the '897 Patent.

41. The '897 Patent is valid and enforceable and enjoys a statutory presumption of validity pursuant to 35 U.S.C. § 282.

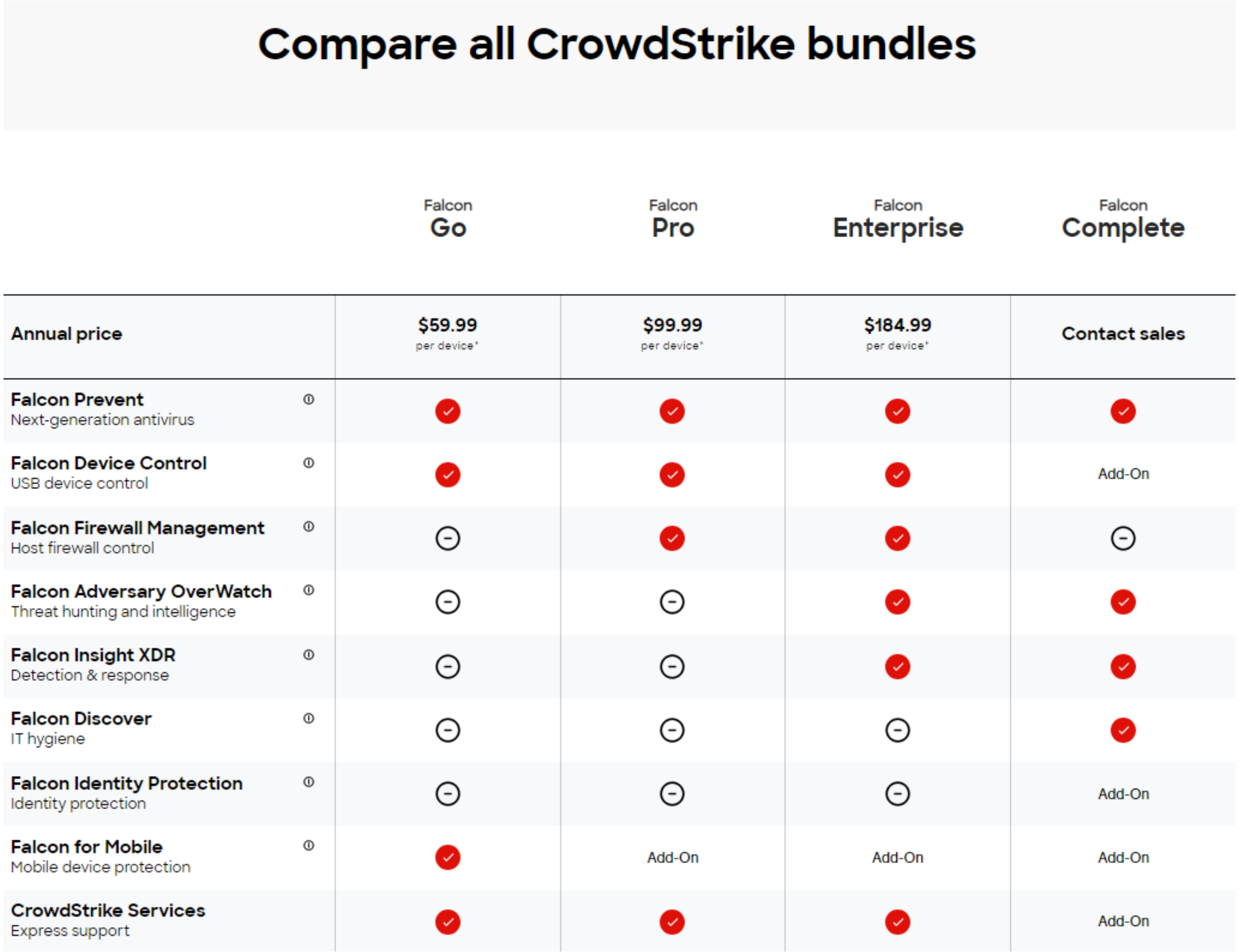
THE ACCUSED PRODUCTS

42. CrowdStrike offers, sells, and uses several products that provide and implement malware detection and endpoint protection platforms for individuals and enterprises and incorporate Plaintiff's patented technologies. These products include the CrowdStrike Falcon Platform, a cloud-based software-as-a-service ("SaaS") for next-generation antivirus ("NGAV") and endpoint detection and response ("EDR").

43. The Falcon Platform is made up of numerous modules that provide antivirus and related SaaS services. These modules are part of and can be added to the base Falcon Platform. Examples of these modules are discussed further below.

44. For example, Falcon Prevent is the core antivirus or NGAV module of the Falcon Platform and is included in every Falcon Platform subscription and bundle as shown by the red

check marks for Falcon Go, Falcon Pro, Falcon Enterprise, and Falcon Complete. Falcon Prevent "[p]rotects against all types of threat, from malware and ransomware to sophisticated attacks."[13]



Compare all CrowdStrike bundles

	Falcon Go	Falcon Pro	Falcon Enterprise	Falcon Complete
Annual price	**$59.99** per device*	**$99.99** per device*	**$184.99** per device*	**Contact sales**
Falcon Prevent Next-generation antivirus ⓘ	✓	✓	✓	✓
Falcon Device Control USB device control ⓘ	✓	✓	✓	Add-On
Falcon Firewall Management Host firewall control ⓘ	⊖	✓	✓	⊖
Falcon Adversary OverWatch Threat hunting and intelligence ⓘ	⊖	⊖	✓	✓
Falcon Insight XDR Detection & response ⓘ	⊖	⊖	✓	✓
Falcon Discover IT hygiene ⓘ	⊖	⊖	⊖	✓
Falcon Identity Protection Identity protection ⓘ	⊖	⊖	⊖	Add-On
Falcon for Mobile Mobile device protection ⓘ	✓	Add-On	Add-On	Add-On
CrowdStrike Services Express support	✓	✓	✓	Add-On

45. As another example, Falcon Exposure Management is a premium Falcon Platform module that replaced Falcon Spotlight and incorporated its functionality, which assesses and remediates vulnerabilities in a computer environment.[14]

46. Falcon Adversary Intelligence, another premium Falcon Platform module, implements extended threat intelligence and dark web monitoring to Falcon Platform customers.

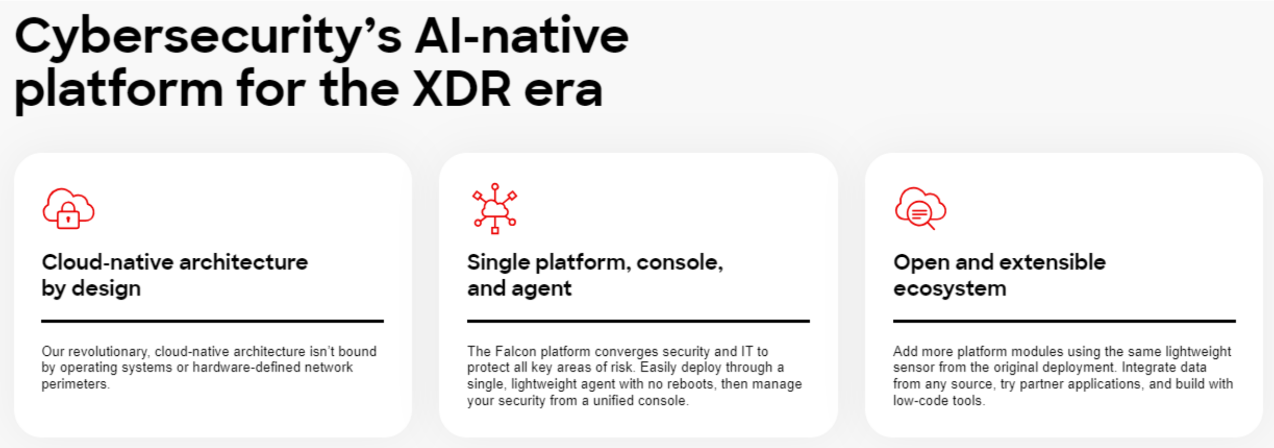
[13] https://www.crowdstrike.com/products/.

[14] https://www.crowdstrike.com/wp-content/uploads/2024/09/falcon-exposure-management-data-sheet.pdf.

Falcon Adversary Intelligence "[d]isrupt[s] adversaries with 24/7 monitoring and real-time alerts to potentially malicious activity across the open, deep and dark web."[15]

47. The Falcon Platform is implemented on endpoint computers using a software called the Falcon sensor or Falcon agent that protects computers and supports the Falcon Platform's cloud infrastructure.[16] On information and belief, the Falcon Platform operates on multiple devices using the Falcon agent including workstations, desktops, laptops, and other traditional end user computer devices, servers, virtual machines, cloud containers, cloud networks, mobile computer devices such as smartphones, and Internet of Things devices.

48. Using a "[s]ingle platform, console, and agent," the Falcon Platform "manage[s] . . . security from a unified console" and is "[e]asily deploy[ed] through a single, lightweight agent with no reboots."[17]



Cybersecurity's AI-native platform for the XDR era

Cloud-native architecture by design

Our revolutionary, cloud-native architecture isn't bound by operating systems or hardware-defined network perimeters.

Single platform, console, and agent

The Falcon platform converges security and IT to protect all key areas of risk. Easily deploy through a single, lightweight agent with no reboots, then manage your security from a unified console.

Open and extensible ecosystem

Add more platform modules using the same lightweight sensor from the original deployment. Integrate data from any source, try partner applications, and build with low-code tools.

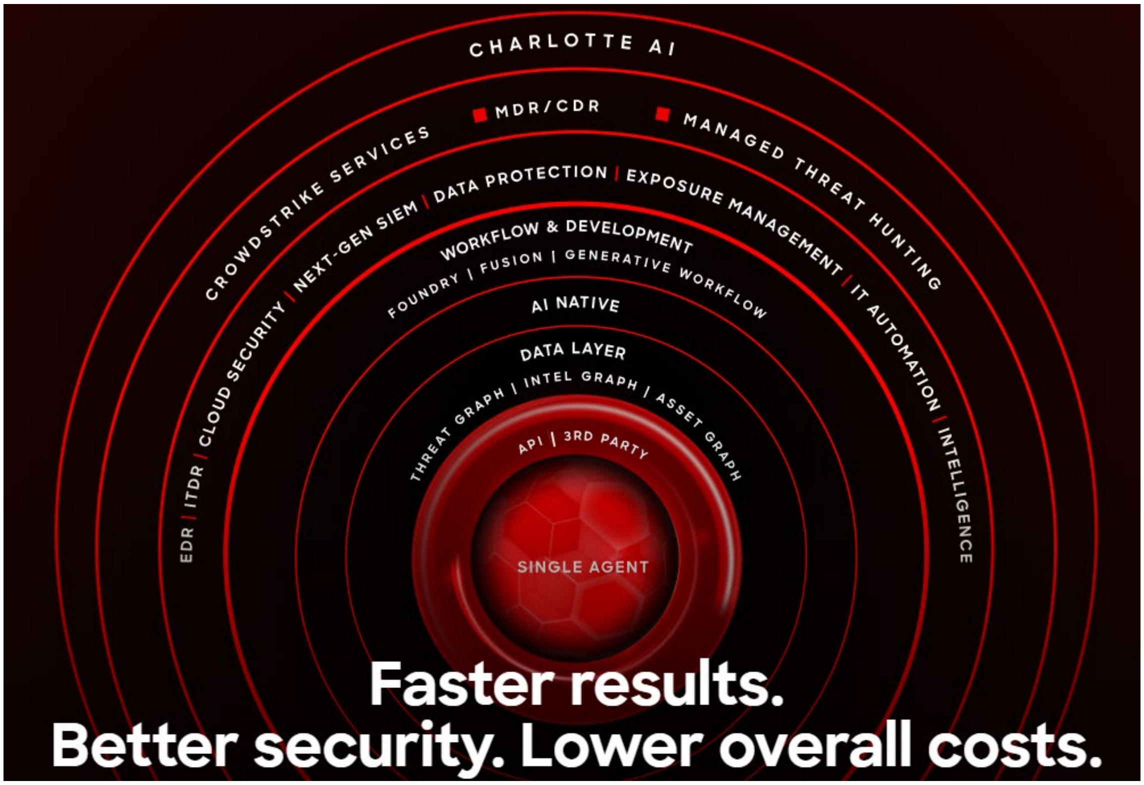
49. As shown below, a "SINGLE AGENT" supports the numerous Falcon Platform modules and features and functionalities including "EDR," "CLOUD SECURITY,"

[15] https://www.crowdstrike.com/wp-content/uploads/2024/04/Data-Sheet-_-Falcon-Adversary-Intelligence.pdf.

[16] https://www.crowdstrike.com/tech-hub/endpoint-security/install-falcon-sensor-for-windows/.

[17] https://www.crowdstrike.com/platform/.

"INTELLIGENCE," and advanced features such as "MDR [managed detection and response]/CDR [cloud detection and response]."


CHARLOTTE AI
MDR/CDR
MANAGED THREAT HUNTING
CROWDSTRIKE SERVICES
EDR | ITDR | CLOUD SECURITY | NEXT-GEN SIEM | DATA PROTECTION | EXPOSURE MANAGEMENT | IT AUTOMATION | INTELLIGENCE
WORKFLOW & DEVELOPMENT
FOUNDRY | FUSION | GENERATIVE WORKFLOW
AI NATIVE
DATA LAYER
THREAT GRAPH | INTEL GRAPH | ASSET GRAPH
API | 3RD PARTY
SINGLE AGENT
Faster results.
Better security. Lower overall costs.

50. On information and belief, Defendants control, operate, and use at least the systems and components in the CrowdStrike Security Cloud.[18] The CrowdStrike Security Cloud network is the foundation upon which the Falcon Platform operates and delivers its security capabilities.

FIRST CAUSE OF ACTION
(INFRINGEMENT OF THE '385 PATENT)

51. Plaintiff incorporates and realleges all of the above paragraphs as though fully set forth herein.

[18] *See* https://www.crowdstrike.com/blog/the-crowdstrike-security-cloud-network-effect/; https://www.crowdstrike.com/tech-hub/?category=endpoint-security/.

52. Defendants are not licensed (expressly or impliedly) or otherwise authorized to make, use, offer for sale, or sell any products or services that embody the inventions of the ’385 Patent.

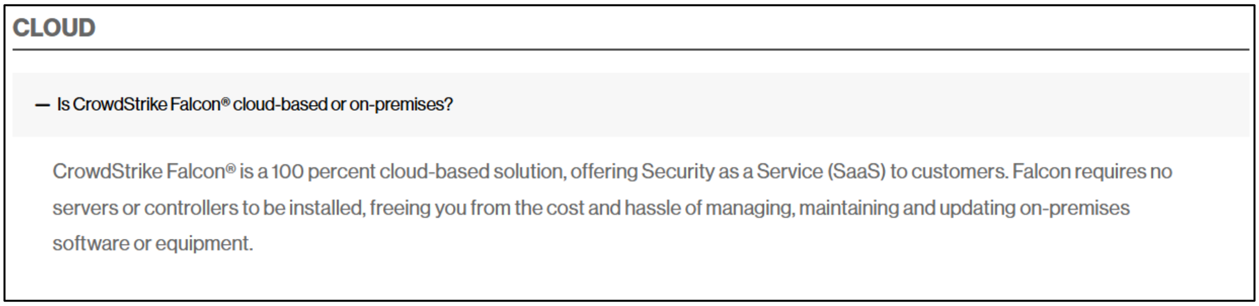
53. Defendants have infringed and continue to infringe, either literally and/or under the doctrine of equivalents, one or more claims of the ’385 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features of the Falcon Platform, at least when used for their ordinary and customary purposes, practice each element of at least claim 8 of the ’385 Patent.

54. Claim 8 of the ’385 Patent recites:

> A method for improving a computing device, the method comprising:
>
> accessing data comprising dark net information associated with a computer system;
>
> obtaining a set of exploits from the dark net information, the set of exploits configured to bypass a security feature of the computer system;
>
> applying an exploit function which takes the set of exploits as input and returns a set of vulnerabilities;
>
> creating a constraint set of vulnerabilities of the computer system from the set of vulnerabilities comprising a minimum set of dependencies to operate the computer system, wherein application of the set of exploits on the computer system comprises determining the effect of the set of exploits on the constraint set of vulnerabilities of the computer system;
>
> analyzing an application associated with the set of exploits on the computer system to detect a particular vulnerability of the constraint set of vulnerabilities of the computer system; and
>
> altering a configuration of the computer system in response to the analysis of the application of the set of exploits to reduce potential damage of a cyberattack.

55. As illustrated in the example below[19], the Falcon Platform embodies a system that includes each element of claim 8 of the ’385 Patent. To the extent that the preamble of claim 8 is limiting, the Falcon Platform perform *a method for improving a computing device*. The Falcon Platform is a cloud-based SaaS that is made up of numerous modules that provide antivirus and related SaaS services to computing devices. For example, Falcon Prevent, which is the core antivirus or NGAV module of the Falcon Platform and is included in every Falcon Platform subscription, “[p]rotects against all types of threat, from malware and ransomware to sophisticated attacks.”[20]

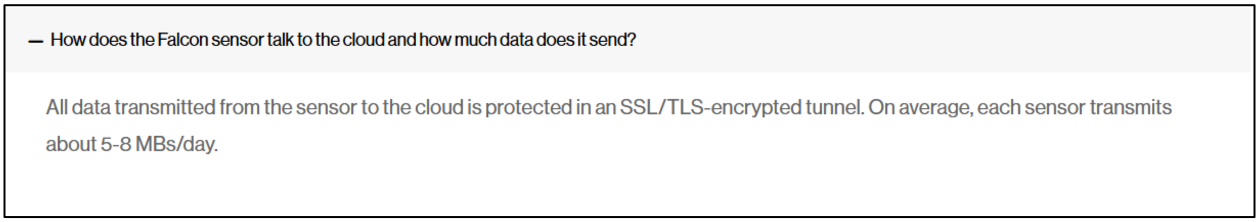
56. The Falcon Platform is “a 100 percent cloud-based solution, offering Security as a Service (SaaS) to customers.” Being cloud-based means that the Falcon Agent (sensor) receives and sends data between an endpoint computer (e.g., server, laptop) and the CrowdStrike Cloud and associated server computers. “All data transmitted from the sensor to the cloud is protected in an SSL/TLS-encrypted tunnel” with an average transmission of “about 5-8 MBs/day” for each sensor.



CLOUD

— Is CrowdStrike Falcon® cloud-based or on-premises?

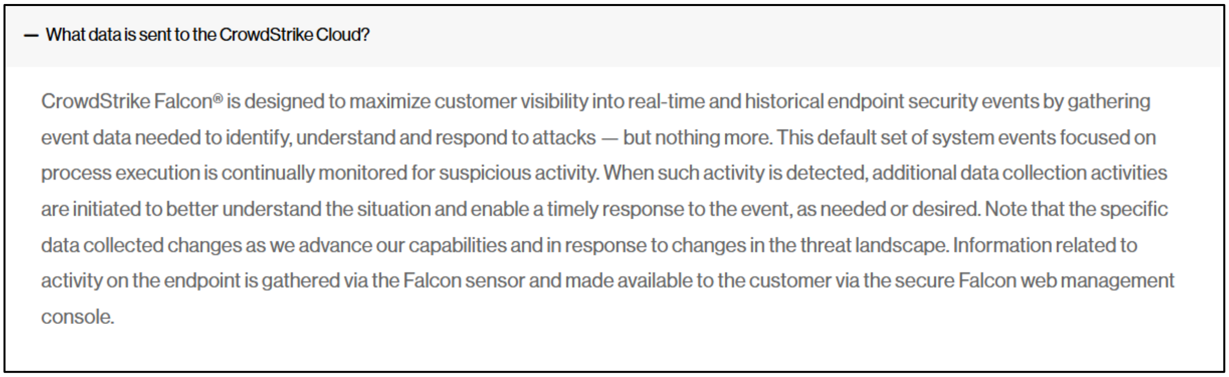
CrowdStrike Falcon® is a 100 percent cloud-based solution, offering Security as a Service (SaaS) to customers. Falcon requires no servers or controllers to be installed, freeing you from the cost and hassle of managing, maintaining and updating on-premises software or equipment.



— How does the Falcon sensor talk to the cloud and how much data does it send?

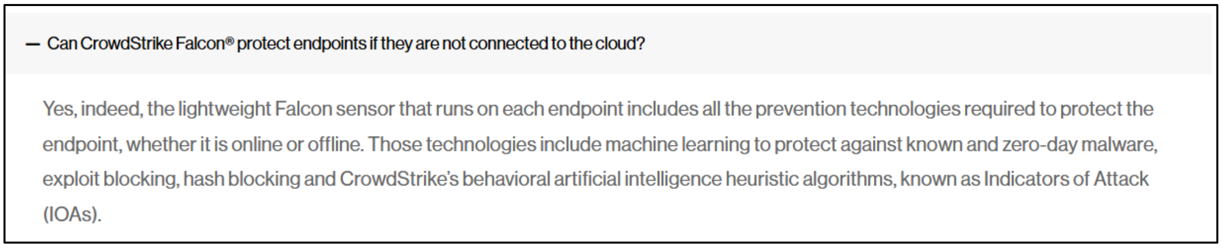
All data transmitted from the sensor to the cloud is protected in an SSL/TLS-encrypted tunnel. On average, each sensor transmits about 5-8 MBs/day.

[19] The following examples are illustrative only and not intended to limit Plaintiff’s right to supplement or modify its allegations regarding the exemplary products or to allege that other CrowdStrike products infringe the ’385 Patent.
[20] https://www.crowdstrike.com/products/.



— What data is sent to the CrowdStrike Cloud?

CrowdStrike Falcon® is designed to maximize customer visibility into real-time and historical endpoint security events by gathering event data needed to identify, understand and respond to attacks — but nothing more. This default set of system events focused on process execution is continually monitored for suspicious activity. When such activity is detected, additional data collection activities are initiated to better understand the situation and enable a timely response to the event, as needed or desired. Note that the specific data collected changes as we advance our capabilities and in response to changes in the threat landscape. Information related to activity on the endpoint is gathered via the Falcon sensor and made available to the customer via the secure Falcon web management console.

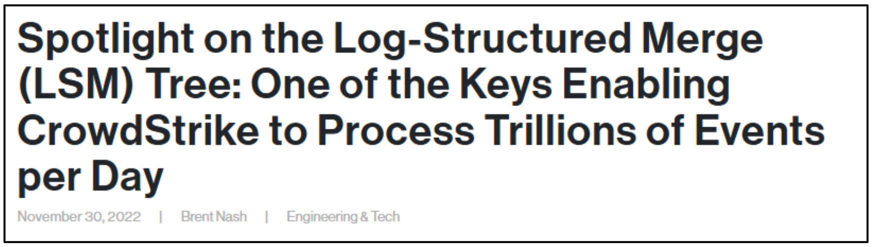


— Can CrowdStrike Falcon® protect endpoints if they are not connected to the cloud?

Yes, indeed, the lightweight Falcon sensor that runs on each endpoint includes all the prevention technologies required to protect the endpoint, whether it is online or offline. Those technologies include machine learning to protect against known and zero-day malware, exploit blocking, hash blocking and CrowdStrike's behavioral artificial intelligence heuristic algorithms, known as Indicators of Attack (IOAs).

[21]

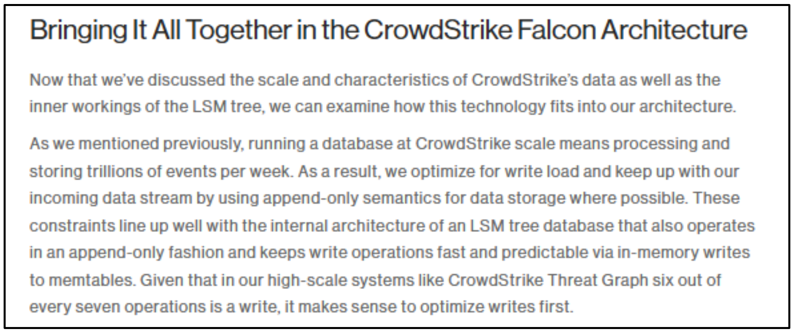
57. Furthermore, the "CrowdStrike Falcon Architecture"—including the CrowdStrike Cloud and CrowdStrike's "database[s]" including "Threat Graph"—"process[] and store[] trillions of events per week." CrowdStrike also states Falcon Platform's lightweight Falcon sensor "consum[es] 1% or less of CPU [central processing unit]" power.



Spotlight on the Log-Structured Merge (LSM) Tree: One of the Keys Enabling CrowdStrike to Process Trillions of Events per Day

November 30, 2022 | Brent Nash | Engineering & Tech

[21] https://www.crowdstrike.com/products/faq/.

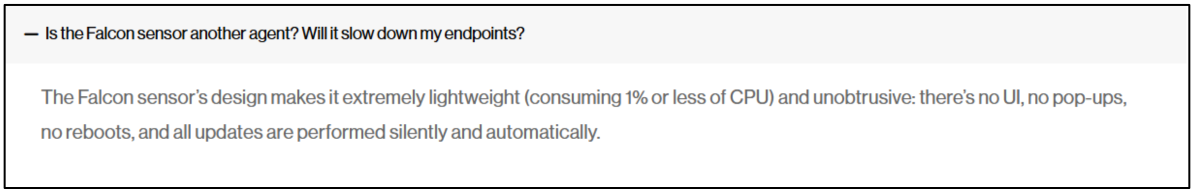


Bringing It All Together in the CrowdStrike Falcon Architecture

Now that we've discussed the scale and characteristics of CrowdStrike's data as well as the inner workings of the LSM tree, we can examine how this technology fits into our architecture.

As we mentioned previously, running a database at CrowdStrike scale means processing and storing trillions of events per week. As a result, we optimize for write load and keep up with our incoming data stream by using append-only semantics for data storage where possible. These constraints line up well with the internal architecture of an LSM tree database that also operates in an append-only fashion and keeps write operations fast and predictable via in-memory writes to memtables. Given that in our high-scale systems like CrowdStrike Threat Graph six out of every seven operations is a write, it makes sense to optimize writes first.

[22]



— Is the Falcon sensor another agent? Will it slow down my endpoints?

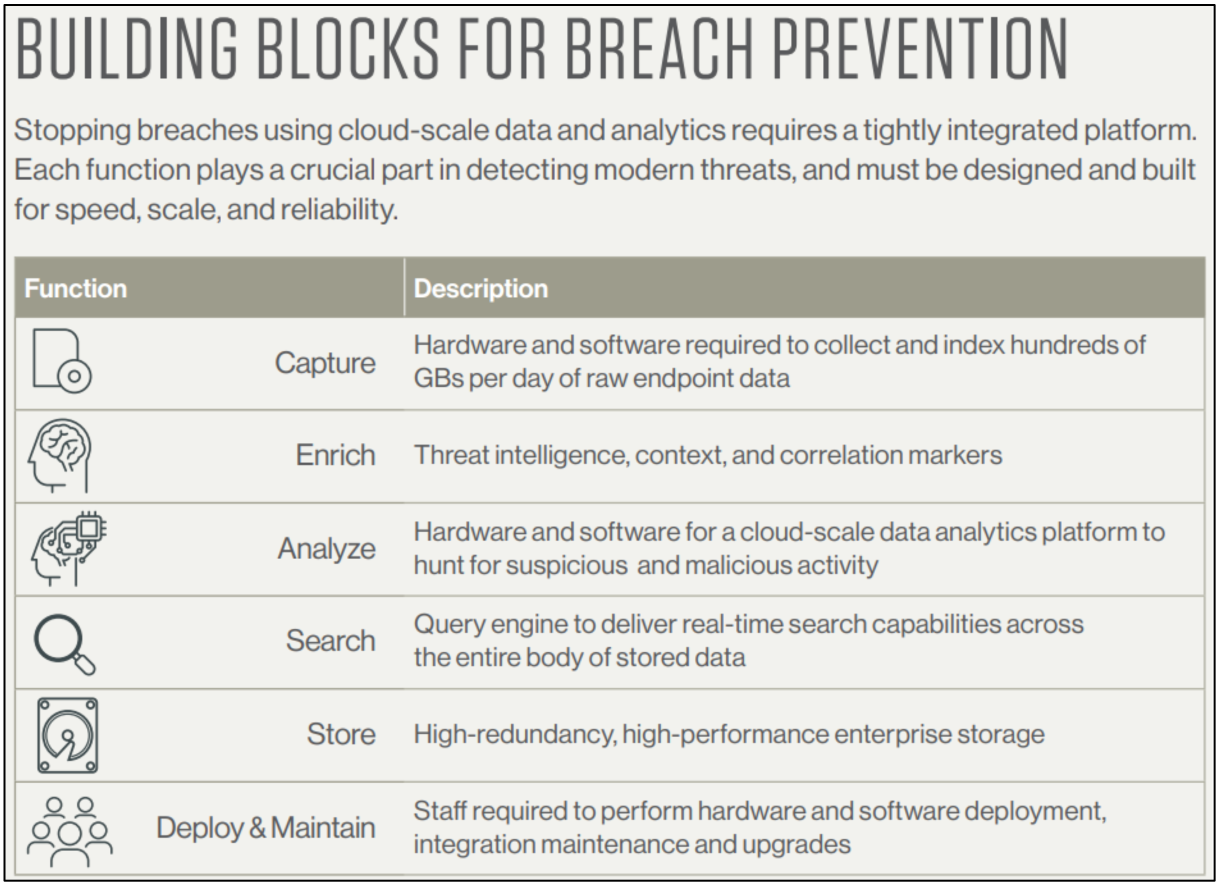
The Falcon sensor's design makes it extremely lightweight (consuming 1% or less of CPU) and unobtrusive: there's no UI, no pop-ups, no reboots, and all updates are performed silently and automatically.

[23]

58. In addition, the Falcon Platform's Threat Graph implements numerous "Function[s]" (configured to store instructions that, when executed) for collecting, analyzing, and storing endpoint telemetry data including "Capture," "Enrich," "Analyze," and "Store." Relatedly, the Falcon Platform implement parameters for "stor[ing] incoming event data" including "Optimize for writes," "No explicit deletes," "Simplicity," and "time-series."

[22] https://www.crowdstrike.com/en-us/blog/how-log-structured-merge-trees-enable-crowdstrike-to-process-trillions-of-events-per-day.

[23] https://www.crowdstrike.com/products/faq/.



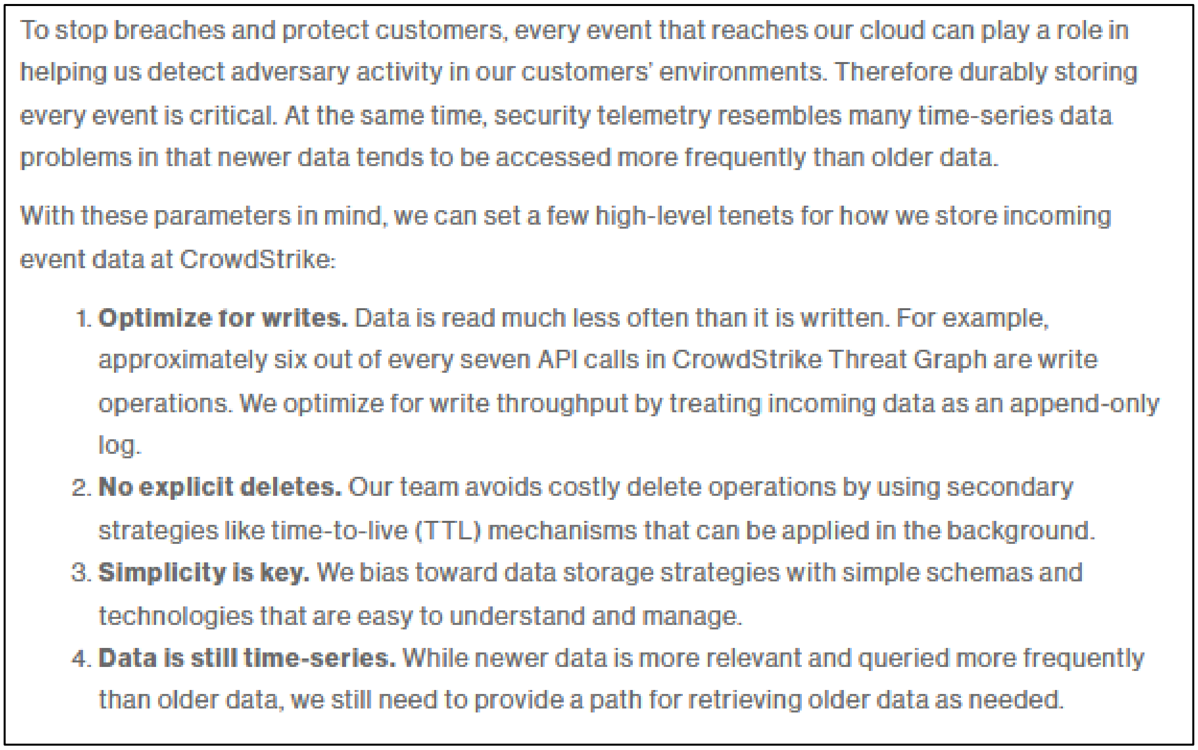
BUILDING BLOCKS FOR BREACH PREVENTION

Stopping breaches using cloud-scale data and analytics requires a tightly integrated platform. Each function plays a crucial part in detecting modern threats, and must be designed and built for speed, scale, and reliability.

Function	Description
Capture	Hardware and software required to collect and index hundreds of GBs per day of raw endpoint data
Enrich	Threat intelligence, context, and correlation markers
Analyze	Hardware and software for a cloud-scale data analytics platform to hunt for suspicious and malicious activity
Search	Query engine to deliver real-time search capabilities across the entire body of stored data
Store	High-redundancy, high-performance enterprise storage
Deploy & Maintain	Staff required to perform hardware and software deployment, integration maintenance and upgrades

[24]

[24] https://www.crowdstrike.com/wp-content/uploads/2019/03/crowdstrike-threat-graph-solution-brief.pdf.



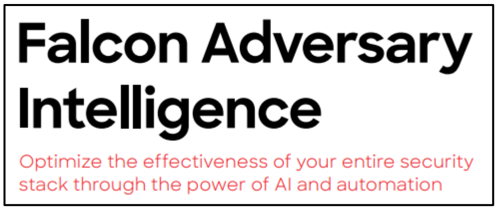
To stop breaches and protect customers, every event that reaches our cloud can play a role in helping us detect adversary activity in our customers' environments. Therefore durably storing every event is critical. At the same time, security telemetry resembles many time-series data problems in that newer data tends to be accessed more frequently than older data.

With these parameters in mind, we can set a few high-level tenets for how we store incoming event data at CrowdStrike:

1. **Optimize for writes.** Data is read much less often than it is written. For example, approximately six out of every seven API calls in CrowdStrike Threat Graph are write operations. We optimize for write throughput by treating incoming data as an append-only log.
2. **No explicit deletes.** Our team avoids costly delete operations by using secondary strategies like time-to-live (TTL) mechanisms that can be applied in the background.
3. **Simplicity is key.** We bias toward data storage strategies with simple schemas and technologies that are easy to understand and manage.
4. **Data is still time-series.** While newer data is more relevant and queried more frequently than older data, we still need to provide a path for retrieving older data as needed.

[25]

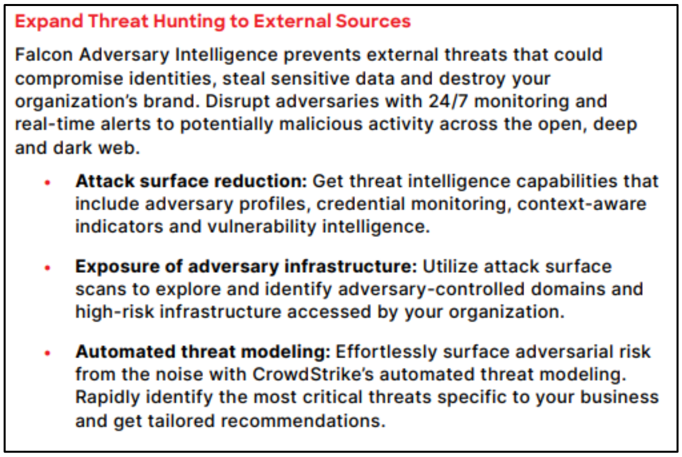
59. The Falcon Platform performs a method that includes *accessing data comprising dark net information associated with a computer system*. For instance, Falcon Adversary Intelligence is a premium Falcon Platform module that implements extended threat intelligence and dark web monitoring to Falcon Platform customers. FAI "[d]isrupt[s] adversaries with 24/7 monitoring and real-time alerts to potentially malicious activity across the open, deep and dark web."



Falcon Adversary Intelligence

Optimize the effectiveness of your entire security stack through the power of AI and automation

[25] https://www.crowdstrike.com/en-us/blog/how-log-structured-merge-trees-enable-crowdstrike-to-process-trillions-of-events-per-day.

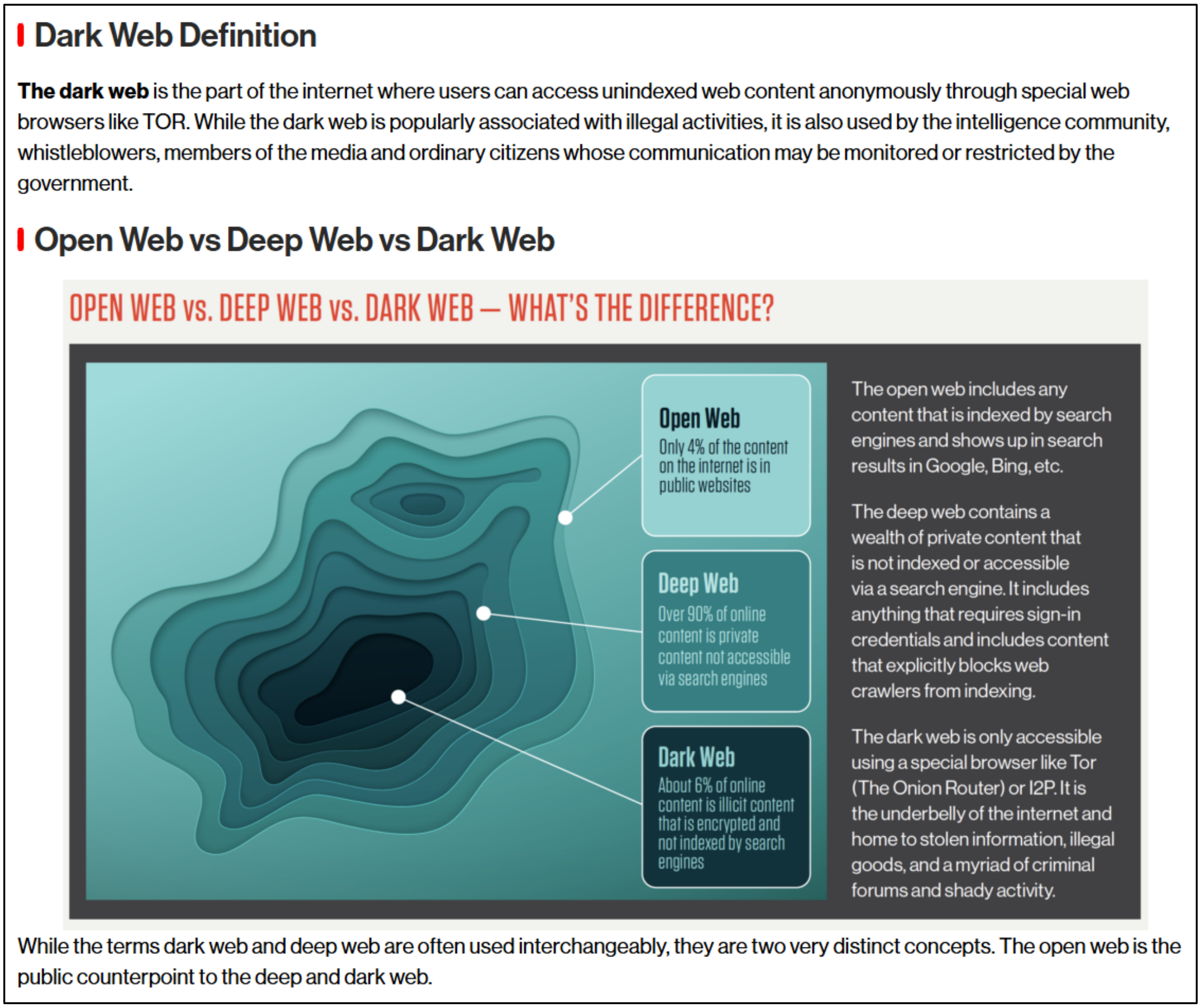


Expand Threat Hunting to External Sources

Falcon Adversary Intelligence prevents external threats that could compromise identities, steal sensitive data and destroy your organization's brand. Disrupt adversaries with 24/7 monitoring and real-time alerts to potentially malicious activity across the open, deep and dark web.

- **Attack surface reduction:** Get threat intelligence capabilities that include adversary profiles, credential monitoring, context-aware indicators and vulnerability intelligence.
- **Exposure of adversary infrastructure:** Utilize attack surface scans to explore and identify adversary-controlled domains and high-risk infrastructure accessed by your organization.
- **Automated threat modeling:** Effortlessly surface adversarial risk from the noise with CrowdStrike's automated threat modeling. Rapidly identify the most critical threats specific to your business and get tailored recommendations.

[26]



Dark Web Definition

The dark web is the part of the internet where users can access unindexed web content anonymously through special web browsers like TOR. While the dark web is popularly associated with illegal activities, it is also used by the intelligence community, whistleblowers, members of the media and ordinary citizens whose communication may be monitored or restricted by the government.

Open Web vs Deep Web vs Dark Web

OPEN WEB vs. DEEP WEB vs. DARK WEB — WHAT'S THE DIFFERENCE?

Open Web
Only 4% of the content on the internet is in public websites
Deep Web
Over 90% of online content is private content not accessible via search engines
Dark Web
About 6% of online content is illicit content that is encrypted and not indexed by search engines

The open web includes any content that is indexed by search engines and shows up in search results in Google, Bing, etc.

The deep web contains a wealth of private content that is not indexed or accessible via a search engine. It includes anything that requires sign-in credentials and includes content that explicitly blocks web crawlers from indexing.

The dark web is only accessible using a special browser like Tor (The Onion Router) or I2P. It is the underbelly of the internet and home to stolen information, illegal goods, and a myriad of criminal forums and shady activity.

While the terms dark web and deep web are often used interchangeably, they are two very distinct concepts. The open web is the public counterpoint to the deep and dark web.

[27]

[26] https://www.crowdstrike.com/wp-content/uploads/2024/04/Data-Sheet-_-Falcon-Adversary-Intelligence.pdf.

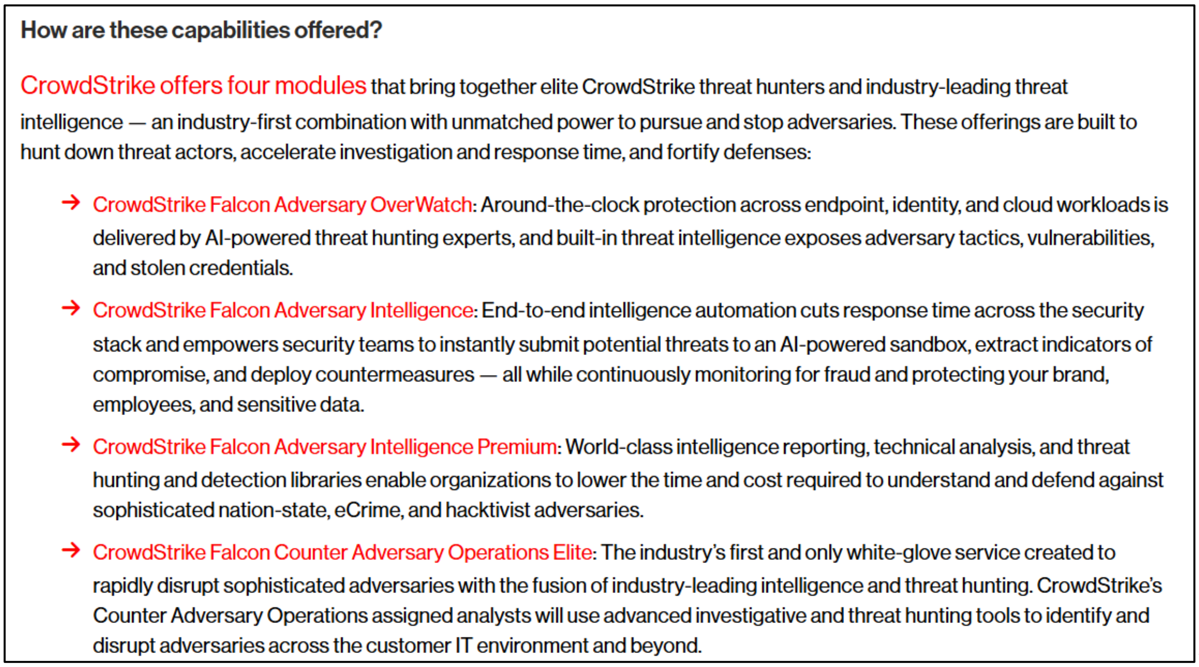
[27] https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/dark-web/.

60. Relatedly, Falcon Adversary Intelligence Premium offers the same benefits as Falcon Adversary Intelligence, plus in-depth technical reports covering adversaries' activities, tools, and tradecraft and pre-tested rules (YARA/SNORT) delivered by CrowdStrike experts. In addition, Falcon Adversary OverWatch implements CrowdStrike's threat-hunting team that, amongst other features, proactively detects adversaries on the dark web.

Falcon Adversary Intelligence Premium

Level up your security team to defeat adversaries

[28]



How are these capabilities offered?

CrowdStrike offers four modules that bring together elite CrowdStrike threat hunters and industry-leading threat intelligence — an industry-first combination with unmatched power to pursue and stop adversaries. These offerings are built to hunt down threat actors, accelerate investigation and response time, and fortify defenses:

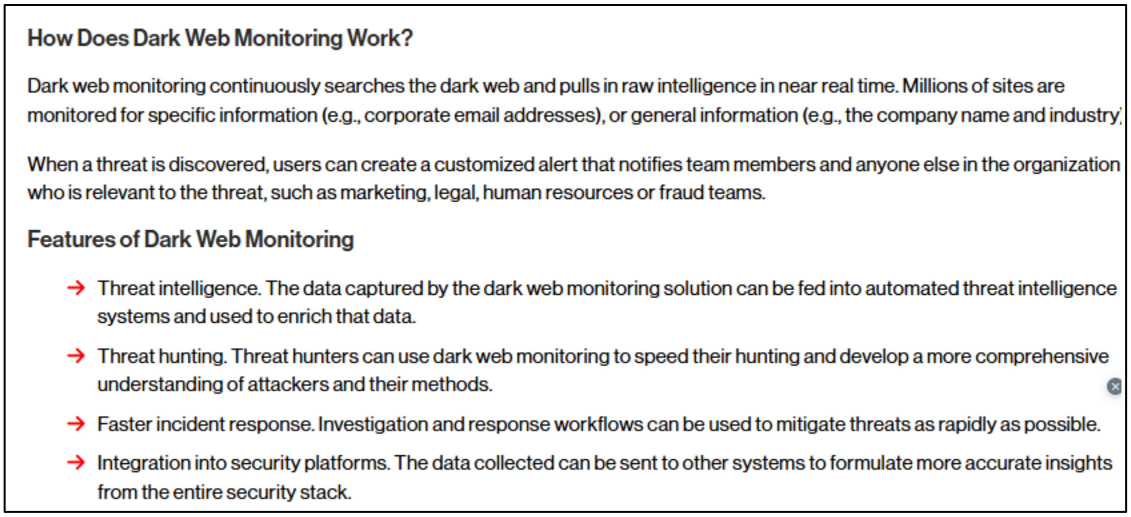
- → CrowdStrike Falcon Adversary OverWatch: Around-the-clock protection across endpoint, identity, and cloud workloads is delivered by AI-powered threat hunting experts, and built-in threat intelligence exposes adversary tactics, vulnerabilities, and stolen credentials.
- → CrowdStrike Falcon Adversary Intelligence: End-to-end intelligence automation cuts response time across the security stack and empowers security teams to instantly submit potential threats to an AI-powered sandbox, extract indicators of compromise, and deploy countermeasures — all while continuously monitoring for fraud and protecting your brand, employees, and sensitive data.
- → CrowdStrike Falcon Adversary Intelligence Premium: World-class intelligence reporting, technical analysis, and threat hunting and detection libraries enable organizations to lower the time and cost required to understand and defend against sophisticated nation-state, eCrime, and hacktivist adversaries.
- → CrowdStrike Falcon Counter Adversary Operations Elite: The industry's first and only white-glove service created to rapidly disrupt sophisticated adversaries with the fusion of industry-leading intelligence and threat hunting. CrowdStrike's Counter Adversary Operations assigned analysts will use advanced investigative and threat hunting tools to identify and disrupt adversaries across the customer IT environment and beyond.

[29]

61. Moreover, CrowdStrike's threat intelligence and hunting team implements "Dark Web Monitoring" to "search[] the dark web and pull[] in raw intelligence in near real time." Dark web websites are "monitored for specific information" and "general information."

[28] https://www.crowdstrike.com/wp-content/uploads/2024/02/falcon-adversary-intelligence-premium-data-sheet.pdf; https://www.crowdstrike.com/platform/threat-intelligence/adversary-overwatch/.

[29] https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/counter-adversary-operations-cao/.



How Does Dark Web Monitoring Work?

Dark web monitoring continuously searches the dark web and pulls in raw intelligence in near real time. Millions of sites are monitored for specific information (e.g., corporate email addresses), or general information (e.g., the company name and industry)

When a threat is discovered, users can create a customized alert that notifies team members and anyone else in the organization who is relevant to the threat, such as marketing, legal, human resources or fraud teams.

Features of Dark Web Monitoring

→ Threat intelligence. The data captured by the dark web monitoring solution can be fed into automated threat intelligence systems and used to enrich that data.

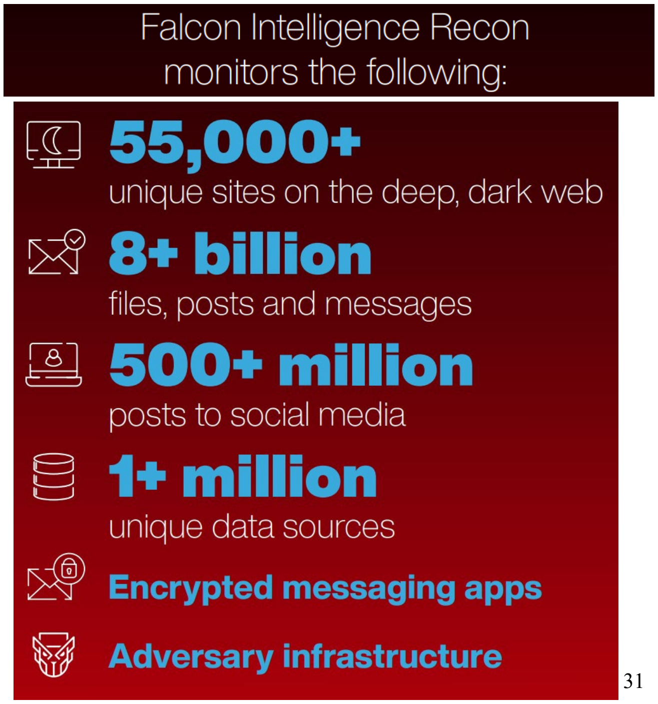
→ Threat hunting. Threat hunters can use dark web monitoring to speed their hunting and develop a more comprehensive understanding of attackers and their methods.

→ Faster incident response. Investigation and response workflows can be used to mitigate threats as rapidly as possible.

→ Integration into security platforms. The data collected can be sent to other systems to formulate more accurate insights from the entire security stack.

[30]

62. CrowdStrike's prior intelligence modules (which Falcon Adversary Intelligence has replaced) also implement deep and dark web monitoring. As an example, Falcon Intelligence Recon monitors "55,000+ unique sites on the deep, dark web," "8+ billion files, posts and messages," and "1+ million unique data sources."



Falcon Intelligence Recon monitors the following:

55,000+ unique sites on the deep, dark web

8+ billion files, posts and messages

500+ million posts to social media

1+ million unique data sources

Encrypted messaging apps

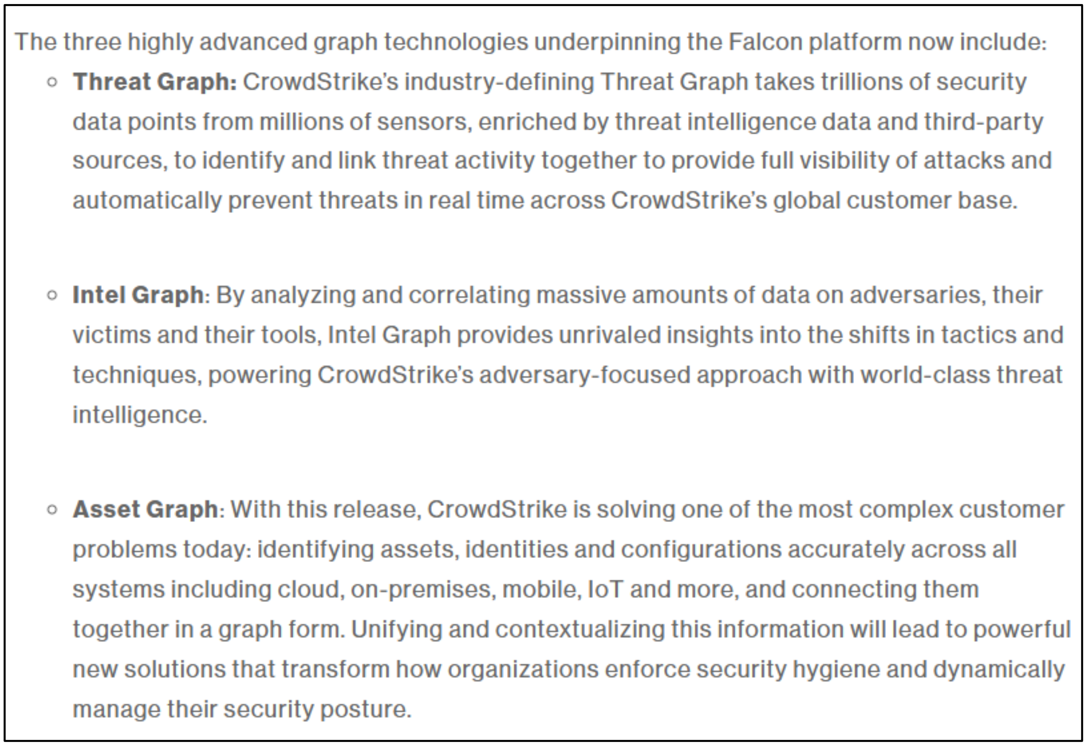
Adversary infrastructure

[31]

[30] https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/dark-web-monitoring/.

[31] https://www.crowdstrike.com/wp-content/uploads/2022/10/falcon-threat-intelligence-recon-infographic.pdf.

63. Furthermore, the Falcon Platform implements "three highly advanced graph [database] technologies" including Threat Graph and Intel Graph. Threat Graph "takes trillions of security data points from millions of sensors" and "identif[ies] and link[s] threat activity together." Intel Graph "analyz[es] and correlat[es] massive amounts of data on adversaries, their victims and their tools" and "power[s] CrowdStrike's adversary-focused approach with world-class threat intelligence."



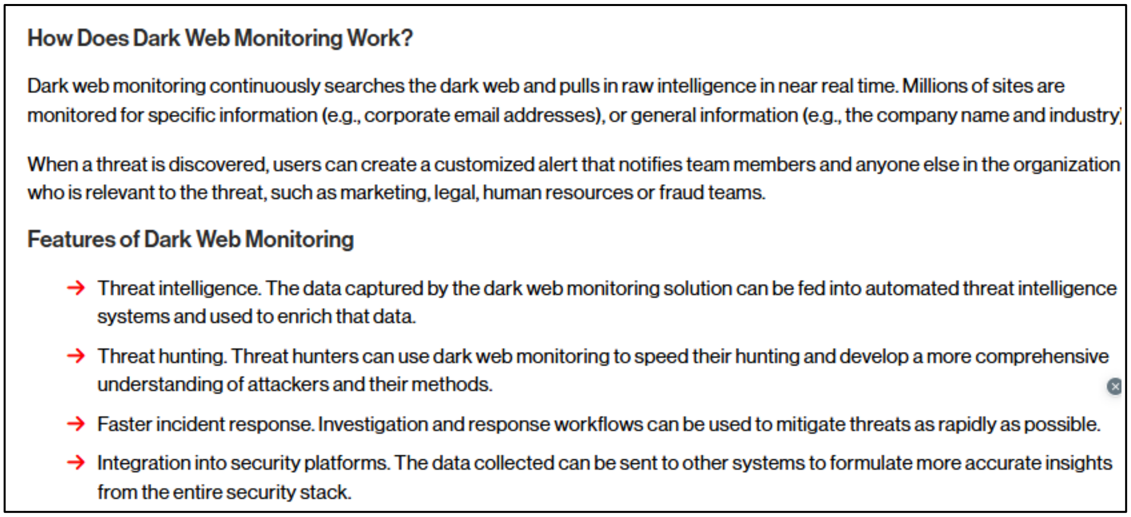
The three highly advanced graph technologies underpinning the Falcon platform now include:

- **Threat Graph:** CrowdStrike's industry-defining Threat Graph takes trillions of security data points from millions of sensors, enriched by threat intelligence data and third-party sources, to identify and link threat activity together to provide full visibility of attacks and automatically prevent threats in real time across CrowdStrike's global customer base.
- **Intel Graph**: By analyzing and correlating massive amounts of data on adversaries, their victims and their tools, Intel Graph provides unrivaled insights into the shifts in tactics and techniques, powering CrowdStrike's adversary-focused approach with world-class threat intelligence.
- **Asset Graph**: With this release, CrowdStrike is solving one of the most complex customer problems today: identifying assets, identities and configurations accurately across all systems including cloud, on-premises, mobile, IoT and more, and connecting them together in a graph form. Unifying and contextualizing this information will lead to powerful new solutions that transform how organizations enforce security hygiene and dynamically manage their security posture.

[32]

64. The Falcon Platform performs a method that includes *obtaining a set of exploits from the dark net information, the set of exploits configured to bypass a security feature of the computer system*. As previously discussed, the Falcon Platform and Falcon Adversary Intelligence monitors the dark web as part of CrowdStrike's counter adversary operations. In addition, Falcon Adversary Intelligence and CrowdStrike's threat hunters implement "dark web monitoring" to "develop a more comprehensive understanding of attackers and their methods."

[32] https://www.crowdstrike.com/en-us/blog/introducing-crowdstrike-asset-graph/.



How Does Dark Web Monitoring Work?

Dark web monitoring continuously searches the dark web and pulls in raw intelligence in near real time. Millions of sites are monitored for specific information (e.g., corporate email addresses), or general information (e.g., the company name and industry)

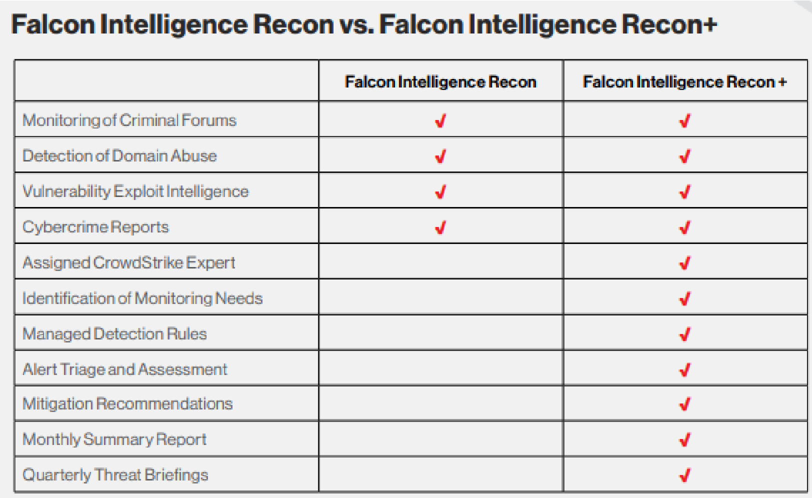
When a threat is discovered, users can create a customized alert that notifies team members and anyone else in the organization who is relevant to the threat, such as marketing, legal, human resources or fraud teams.

Features of Dark Web Monitoring

- → Threat intelligence. The data captured by the dark web monitoring solution can be fed into automated threat intelligence systems and used to enrich that data.
- → Threat hunting. Threat hunters can use dark web monitoring to speed their hunting and develop a more comprehensive understanding of attackers and their methods.
- → Faster incident response. Investigation and response workflows can be used to mitigate threats as rapidly as possible.
- → Integration into security platforms. The data collected can be sent to other systems to formulate more accurate insights from the entire security stack.

[33]

65. In an example from the prior Falcon Platform Falcon Intelligence module Falcon Intelligence Recon and Falcon Intelligence Recon+ both "Monitored Criminal Forums" (obtaining a set of exploits from the dark net information) and implemented "Vulnerability Exploit Intelligence" (the set of exploits configured to penetrate the computer system).



Falcon Intelligence Recon vs. Falcon Intelligence Recon+

	Falcon Intelligence Recon	Falcon Intelligence Recon +
Monitoring of Criminal Forums	✓	✓
Detection of Domain Abuse	✓	✓
Vulnerability Exploit Intelligence	✓	✓
Cybercrime Reports	✓	✓
Assigned CrowdStrike Expert		✓
Identification of Monitoring Needs		✓
Managed Detection Rules		✓
Alert Triage and Assessment		✓
Mitigation Recommendations		✓
Monthly Summary Report		✓
Quarterly Threat Briefings		✓

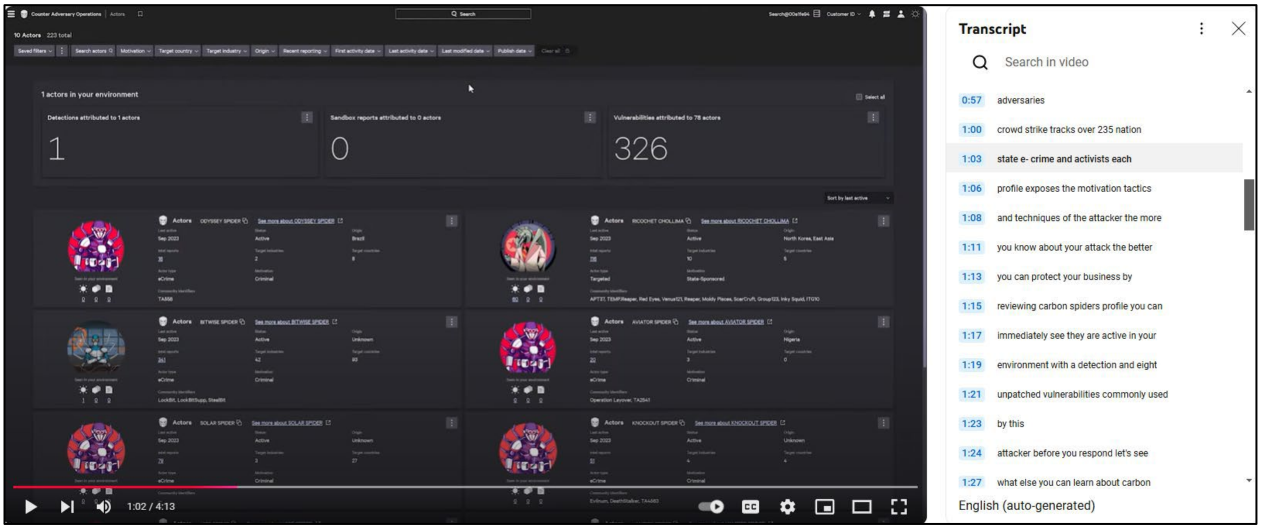
[34]

66. The Falcon Platform embodies a method that includes *applying an exploit function which takes the set of exploits as input and returns a set of vulnerabilities*. As part of Falcon

[33] https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/dark-web-monitoring/.

[34] https://www.crowdstrike.com/wp-content/uploads/2023/12/crowdstrike-falcon-intelligence-recon-plus.pdf.

Adversary Intelligence, "CrowdStrike tracks over 235 nation-state e-crime and activists." In the example shown below, 326 "Vulnerabilities" (and returns a set of vulnerabilities) are "attributed to 78 actors" (applying an exploit function which takes the set of exploits as input). "Community identifiers" such as "LockBit, LockBitSupp, StealBit" (applying an exploit function which takes the set of exploits as input) for eCrime actor "BITWISE SPIDER." As shown, Falcon Adversary Intelligence connects specific actors and known techniques such as exploits with associated vulnerabilities.



Transcript

Search in video

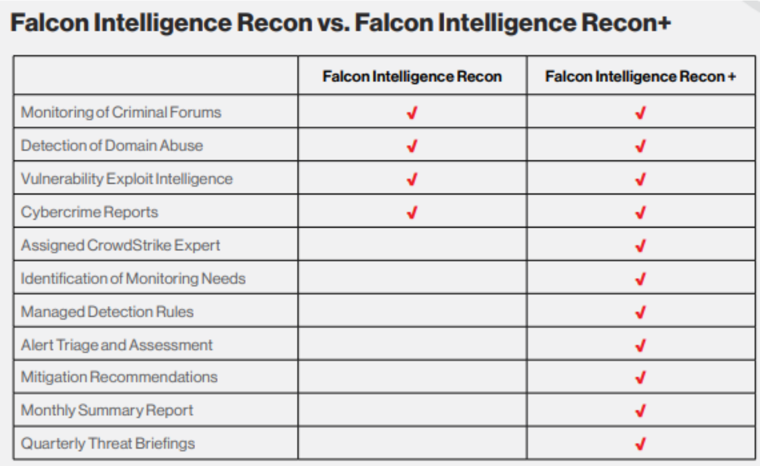
0:57 adversaries
1:00 crowd strike tracks over 235 nation
1:03 state e- crime and activists each
1:06 profile exposes the motivation tactics
1:08 and techniques of the attacker the more
1:11 you know about your attack the better
1:13 you can protect your business by
1:15 reviewing carbon spiders profile you can
1:17 immediately see they are active in your
1:19 environment with a detection and eight
1:21 unpatched vulnerabilities commonly used
1:23 by this
1:24 attacker before you respond let's see
1:27 what else you can learn about carbon

English (auto-generated)

[35]

67. In an example from the prior Falcon Intelligence module, Falcon Intelligence Recon and Falcon Intelligence Recon+ both implement "Vulnerability Exploit Intelligence"

[35] https://www.youtube.com/watch?v=RrKQN8x2Ldc.

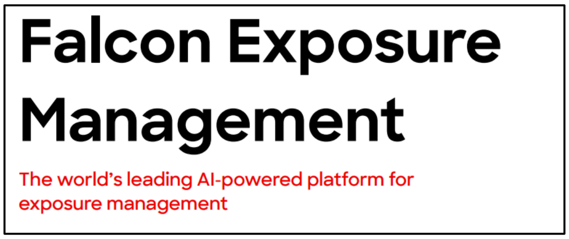


Falcon Intelligence Recon vs. Falcon Intelligence Recon+

	Falcon Intelligence Recon	Falcon Intelligence Recon +
Monitoring of Criminal Forums	✓	✓
Detection of Domain Abuse	✓	✓
Vulnerability Exploit Intelligence	✓	✓
Cybercrime Reports	✓	✓
Assigned CrowdStrike Expert		✓
Identification of Monitoring Needs		✓
Managed Detection Rules		✓
Alert Triage and Assessment		✓
Mitigation Recommendations		✓
Monthly Summary Report		✓
Quarterly Threat Briefings		✓

[36]

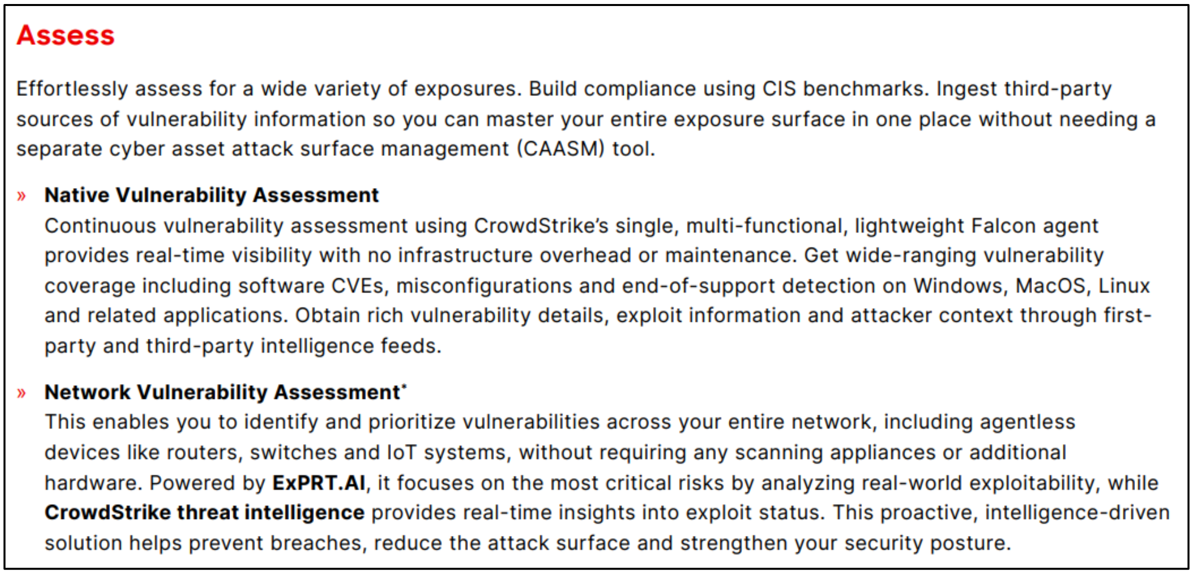
68. In a related example, the Falcon Exposure Management module, another premium Falcon Platform module, assesses and remediates vulnerabilities in a computer environment. Falcon Exposure Management's "Native Vulnerability Assessment . . . [o]btain[s] rich vulnerability details, exploit information and attacker context through first-party and third-party intelligence feeds." The "Network Vulnerability Assessment" uses ExPRT.AI (the Expert Prediction Rating artificial intelligence model) to focus on critical risks "by analyzing real-world exploitability" and CrowdStrike threat intelligence for "real-time insights into exploit status." Moreover, ExPRT.AI is a "dynamic AI model trained on CrowdStrike's exploit intelligence and real-life detection events" that "narrows down crucial vulnerabilities" and an "Active Adversary Context" "industry-leading threat intelligence" to "pinpoint[] and correlate[] vulnerabilities with adversaries."



Falcon Exposure Management

The world's leading AI-powered platform for exposure management

[36] https://www.crowdstrike.com/wp-content/uploads/2023/12/crowdstrike-falcon-intelligence-recon-plus.pdf.

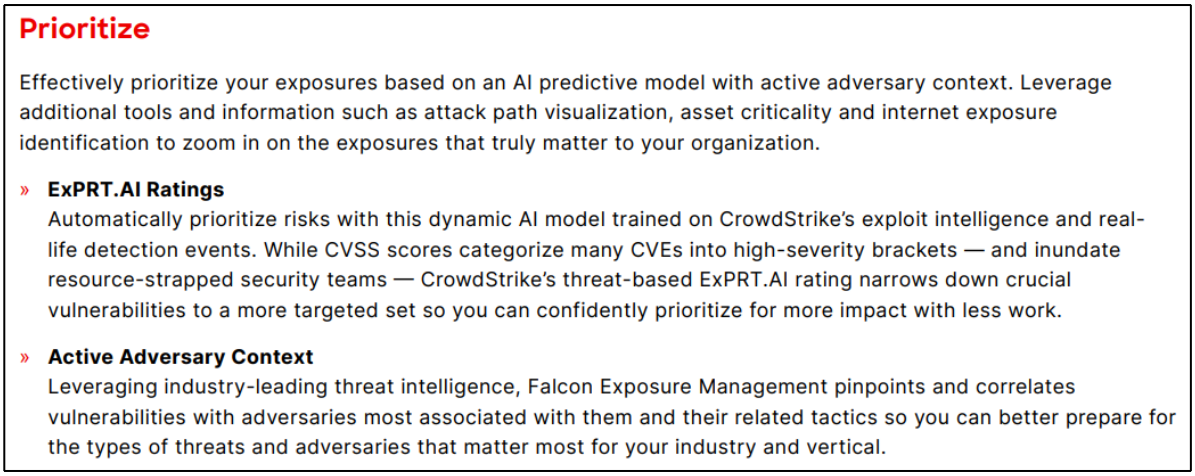


Assess

Effortlessly assess for a wide variety of exposures. Build compliance using CIS benchmarks. Ingest third-party sources of vulnerability information so you can master your entire exposure surface in one place without needing a separate cyber asset attack surface management (CAASM) tool.

» **Native Vulnerability Assessment**
Continuous vulnerability assessment using CrowdStrike's single, multi-functional, lightweight Falcon agent provides real-time visibility with no infrastructure overhead or maintenance. Get wide-ranging vulnerability coverage including software CVEs, misconfigurations and end-of-support detection on Windows, MacOS, Linux and related applications. Obtain rich vulnerability details, exploit information and attacker context through first-party and third-party intelligence feeds.

» **Network Vulnerability Assessment***
This enables you to identify and prioritize vulnerabilities across your entire network, including agentless devices like routers, switches and IoT systems, without requiring any scanning appliances or additional hardware. Powered by **ExPRT.AI**, it focuses on the most critical risks by analyzing real-world exploitability, while **CrowdStrike threat intelligence** provides real-time insights into exploit status. This proactive, intelligence-driven solution helps prevent breaches, reduce the attack surface and strengthen your security posture.



Prioritize

Effectively prioritize your exposures based on an AI predictive model with active adversary context. Leverage additional tools and information such as attack path visualization, asset criticality and internet exposure identification to zoom in on the exposures that truly matter to your organization.

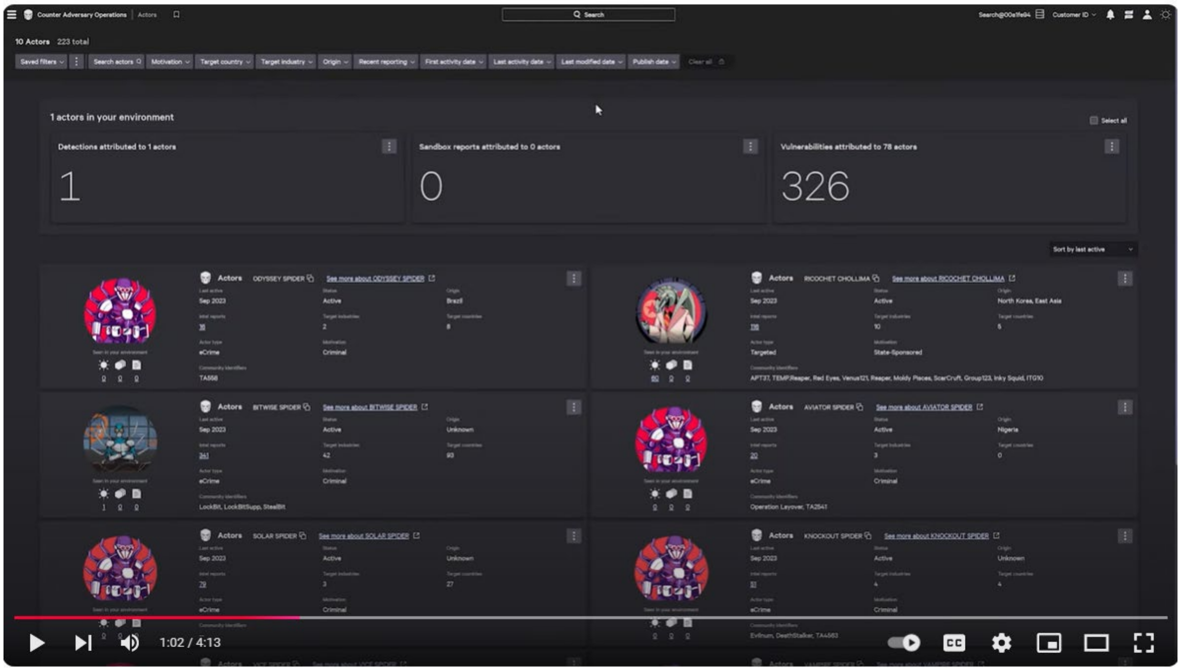
» **ExPRT.AI Ratings**
Automatically prioritize risks with this dynamic AI model trained on CrowdStrike's exploit intelligence and real-life detection events. While CVSS scores categorize many CVEs into high-severity brackets — and inundate resource-strapped security teams — CrowdStrike's threat-based ExPRT.AI rating narrows down crucial vulnerabilities to a more targeted set so you can confidently prioritize for more impact with less work.

» **Active Adversary Context**
Leveraging industry-leading threat intelligence, Falcon Exposure Management pinpoints and correlates vulnerabilities with adversaries most associated with them and their related tactics so you can better prepare for the types of threats and adversaries that matter most for your industry and vertical.

[37]

69. The Falcon Platform performs a method that includes *creating a constraint set of vulnerabilities of the computer system from the set of vulnerabilities comprising a minimum set of dependencies to operate the computer system*. For instance, Falcon Adversary Intelligence is demonstrated below having detected 326 "Vulnerabilities attributed to 78 actors" (creating a constraint set of the computer system from the set of vulnerabilities) based on a customer's computer "environment" (the constraint set comprising a minimum set of dependencies to operate the computer system).

[37] https://www.crowdstrike.com/wp-content/uploads/2024/09/falcon-exposure-management-data-sheet.pdf.



Counter Adversary Operations | Actors

10 Actors 223 total

1 actors in your environment

Detections attributed to 1 actors
1

Sandbox reports attributed to 0 actors
0

Vulnerabilities attributed to 78 actors
326

Actors ODYSSEY SPIDER — See more about ODYSSEY SPIDER
Last active: Sep 2023 | Status: Active | Origin: Brazil
Intel reports: 16 | Target industries: 2 | Target countries: 8
Actor type: eCrime | Motivation: Criminal
Community identifiers: TA558
Seen in your environment: 0 0 0

Actors RICOCHET CHOLLIMA — See more about RICOCHET CHOLLIMA
Last active: Sep 2023 | Status: Active | Origin: North Korea, East Asia
Intel reports: 116 | Target industries: 10 | Target countries: 5
Actor type: Targeted | Motivation: State-Sponsored
Community identifiers: APT37, TEMP.Reaper, Red Eyes, Venus121, Reaper, Moldy Pisces, ScarCruft, Group123, Inky Squid, ITG10
Seen in your environment: 60 0 0

Actors BITWISE SPIDER — See more about BITWISE SPIDER
Last active: Sep 2023 | Status: Active | Origin: Unknown
Intel reports: 341 | Target industries: 42 | Target countries: 93
Actor type: eCrime | Motivation: Criminal
Community identifiers: LockBit, LockBitSupp, StealBit
Seen in your environment: 1 0 0

Actors AVIATOR SPIDER — See more about AVIATOR SPIDER
Last active: Sep 2023 | Status: Active | Origin: Nigeria
Intel reports: 20 | Target industries: 3 | Target countries: 0
Actor type: eCrime | Motivation: Criminal
Community identifiers: Operation Layover, TA2541
Seen in your environment: 0 0 0

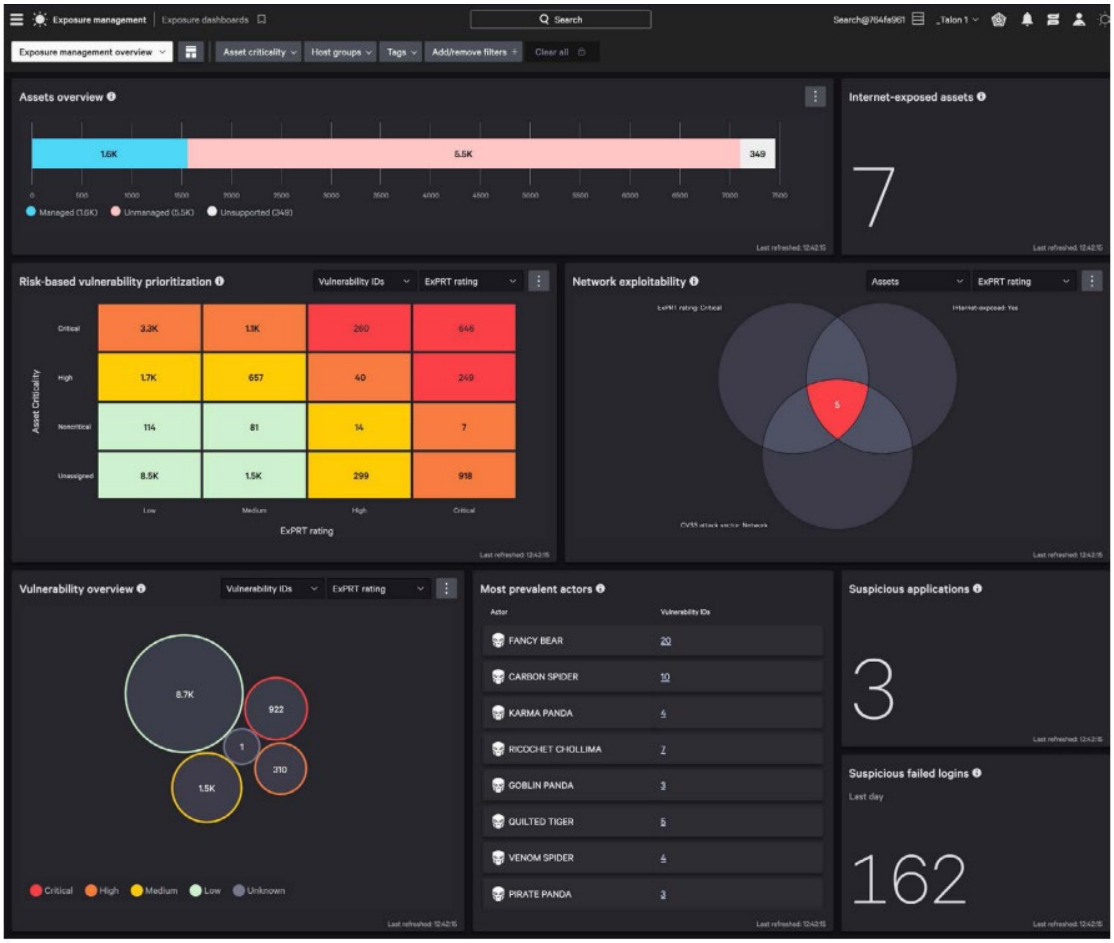
Actors SOLAR SPIDER — See more about SOLAR SPIDER
Last active: Sep 2023 | Status: Active | Origin: Unknown
Intel reports: 79 | Target industries: 3 | Target countries: 27
Actor type: eCrime | Motivation: Criminal

Actors KNOCKOUT SPIDER — See more about KNOCKOUT SPIDER
Last active: Sep 2023 | Status: Active | Origin: Unknown
Intel reports: 31 | Target industries: 4 | Target countries: 4
Actor type: eCrime | Motivation: Criminal
Community identifiers: Evilnum, DeathStalker, TA4563

[38]

70. In addition, the Falcon Exposure Management dashboard is demonstrated below managing “1.6K” assets with 7 “Internet-exposed assets” (the constraint set comprising a minimum set of dependencies to operate the computer system) and “Vulnerability IDs” based on “prevalent actors” such as “FANCY BEAR” (20) and “CARBON SPIDER” (10) (creating a constraint set of the computer system from the set of vulnerabilities).

[38] https://www.youtube.com/watch?v=RrKQN8x2Ldc.



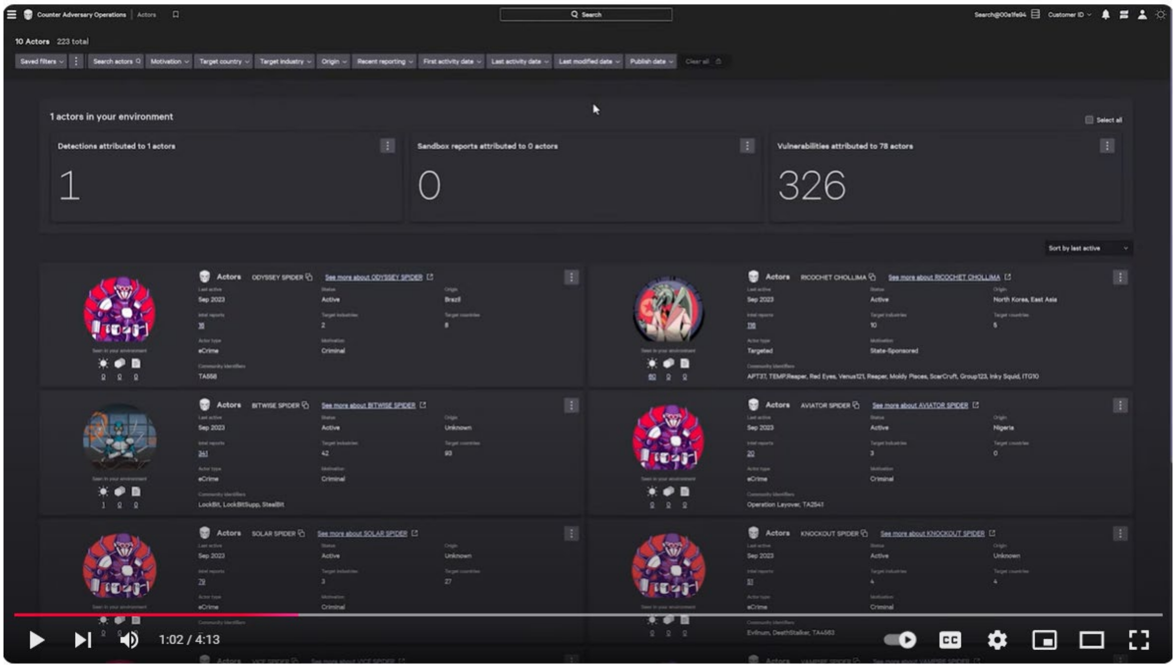
	Low	Medium	High	Critical
Critical	3.3K	1.1K	260	646
High	1.7K	657	40	249
Noncritical	114	81	14	7
Unassigned	8.5K	1.5K	299	918

Actor	Vulnerability IDs
FANCY BEAR	20
CARBON SPIDER	10
KARMA PANDA	4
RICOCHET CHOLLIMA	7
GOBLIN PANDA	3
QUILTED TIGER	5
VENOM SPIDER	4
PIRATE PANDA	3

Falcon Exposure Management unified main dashboard [39]

71. The Falcon Platform performs a method that includes *wherein application of the set of exploits on the computer system comprises determining the effect of the set of exploits on the constraint set of vulnerabilities of the computer system*. As previously discussed, Falcon Adversary Intelligence is demonstrated below having 326 "Vulnerabilities attributed to 78 actors" based on a customer's computer "environment."

[39] https://www.crowdstrike.com/wp-content/uploads/2024/09/falcon-exposure-management-data-sheet.pdf.



10 Actors 223 total

1 actors in your environment

Detections attributed to 1 actors: 1

Sandbox reports attributed to 0 actors: 0

Vulnerabilities attributed to 78 actors: 326

Actors ODYSSEY SPIDER — See more about ODYSSEY SPIDER
Last active: Sep 2023 | Status: Active | Origin: Brazil
Intel reports: 16 | Target industries: 2 | Target countries: 8
Actor type: eCrime | Motivation: Criminal
Community identifiers: TA558
Seen in your environment: 0 0 0

Actors RICOCHET CHOLLIMA — See more about RICOCHET CHOLLIMA
Last active: Sep 2023 | Status: Active | Origin: North Korea, East Asia
Intel reports: 116 | Target industries: 10 | Target countries: 5
Actor type: Targeted | Motivation: State-Sponsored
Community identifiers: APT37, TEMP.Reaper, Red Eyes, Venus121, Reaper, Moldy Pisces, ScarCruft, Group123, Inky Squid, ITG10
Seen in your environment: 60 0 0

Actors BITWISE SPIDER — See more about BITWISE SPIDER
Last active: Sep 2023 | Status: Active | Origin: Unknown
Intel reports: 341 | Target industries: 42 | Target countries: 93
Actor type: eCrime | Motivation: Criminal
Community identifiers: LockBit, LockBitSupp, StealBit
Seen in your environment: 1 0 0

Actors AVIATOR SPIDER — See more about AVIATOR SPIDER
Last active: Sep 2023 | Status: Active | Origin: Nigeria
Intel reports: 20 | Target industries: 3 | Target countries: 0
Actor type: eCrime | Motivation: Criminal
Community identifiers: Operation Layover, TA2541
Seen in your environment: 0 0 0

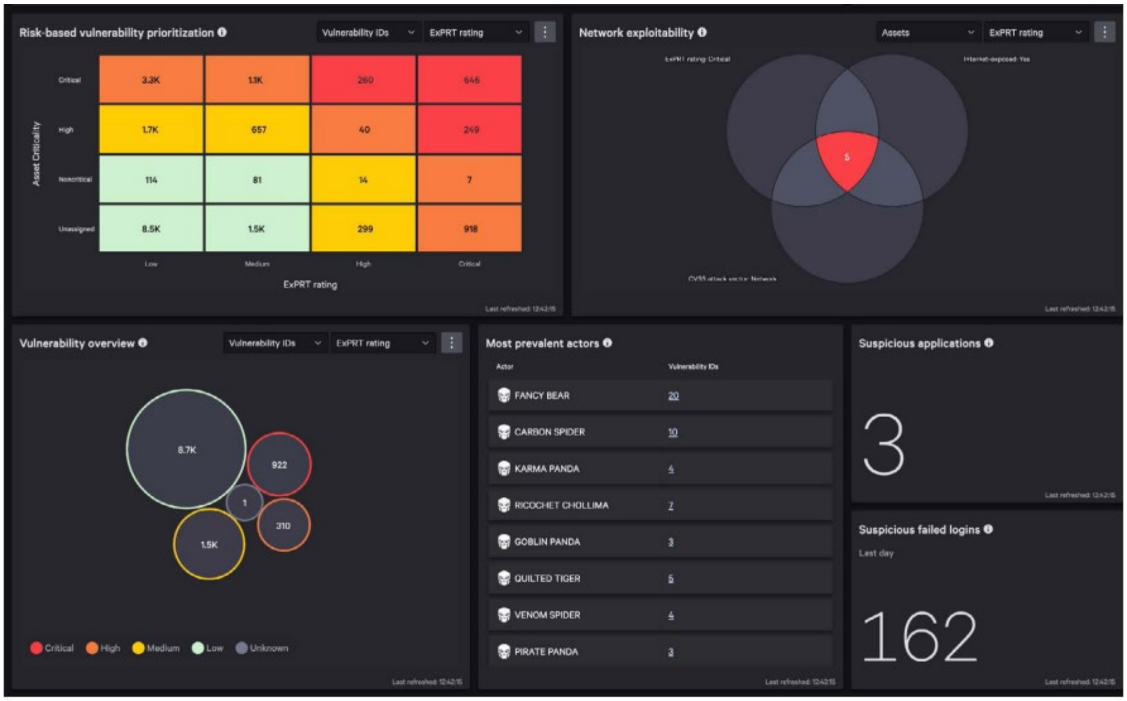
Actors SOLAR SPIDER — See more about SOLAR SPIDER
Last active: Sep 2023 | Status: Active | Origin: Unknown
Intel reports: 79 | Target industries: 3 | Target countries: 27
Actor type: eCrime | Motivation: Criminal
Seen in your environment: 0 0 0

Actors KNOCKOUT SPIDER — See more about KNOCKOUT SPIDER
Last active: Sep 2023 | Status: Active | Origin: Unknown
Intel reports: 51 | Target industries: 4 | Target countries: 4
Actor type: eCrime | Motivation: Criminal
Community identifiers: Evilnum, DeathStalker, TA4563
Seen in your environment: 0 0 0

[40]

72. In addition, the Falcon Exposure Management dashboard is demonstrated displaying "Vulnerability IDs" based on "prevalent actors" such as "FANCY BEAR" (20) and "CARBON SPIDER" (10) as well as 922 "Critical" "Vulnerability IDs" based on "ExPRT rating."

[40] https://www.youtube.com/watch?v=RrKQN8x2Ldc.



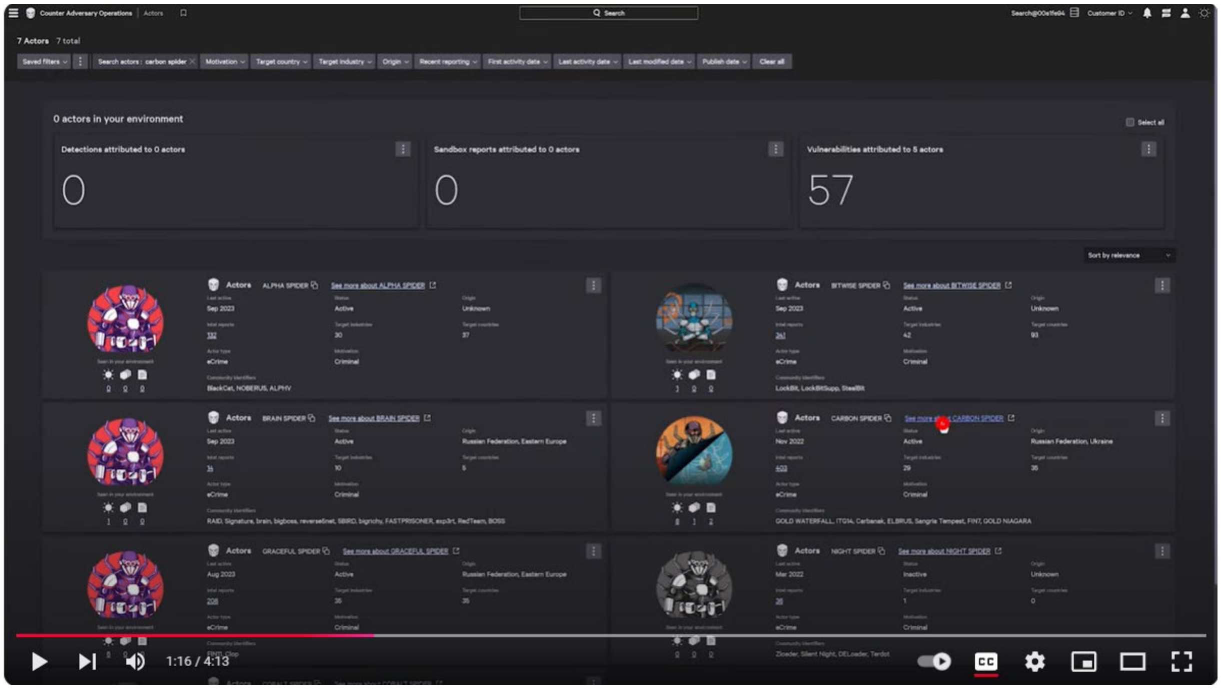
	Low	Medium	High	Critical
Critical	3.3K	1.1K	260	646
High	1.7K	657	40	249
Noncritical	114	81	14	7
Unassigned	8.5K	1.5K	299	918

Actor	Vulnerability IDs
FANCY BEAR	20
CARBON SPIDER	10
KARMA PANDA	4
RICOCHET CHOLLIMA	7
GOBLIN PANDA	3
QUILTED TIGER	5
VENOM SPIDER	4
PIRATE PANDA	3

Falcon Exposure Management unified main dashboard [41]

73. The Falcon Platform performs a method that includes *analyzing an application associated with the set of exploits on the computer system to detect a particular vulnerability of the constraint set of vulnerabilities of the computer system*. In the example shown below, by clicking on the profile for criminal group "CARBON SPIDER" (analyzing the application of the set of exploits on the computer system), Falcon Adversary Intelligence of the Falcon Platform reveals "Actor activity" that includes 1 "Endpoint detections" and 8 "Vulnerabilities" (to detect a particular vulnerability of the computer system) detected on computers protected by the Falcon Platform as well as 30,940 "Total indicators."

[41] https://www.crowdstrike.com/wp-content/uploads/2024/09/falcon-exposure-management-data-sheet.pdf.



Counter Adversary Operations | Actors

7 Actors 7 total

0 actors in your environment

Detections attributed to 0 actors: 0

Sandbox reports attributed to 0 actors: 0

Vulnerabilities attributed to 5 actors: 57

Actors ALPHA SPIDER — See more about ALPHA SPIDER
Last active: Sep 2023 | Status: Active | Origin: Unknown
Intel reports: 132 | Target industries: 30 | Target countries: 37
Actor type: eCrime | Motivation: Criminal
Community identifiers: BlackCat, NOBERUS, ALPHV
Seen in your environment: 0 0 0

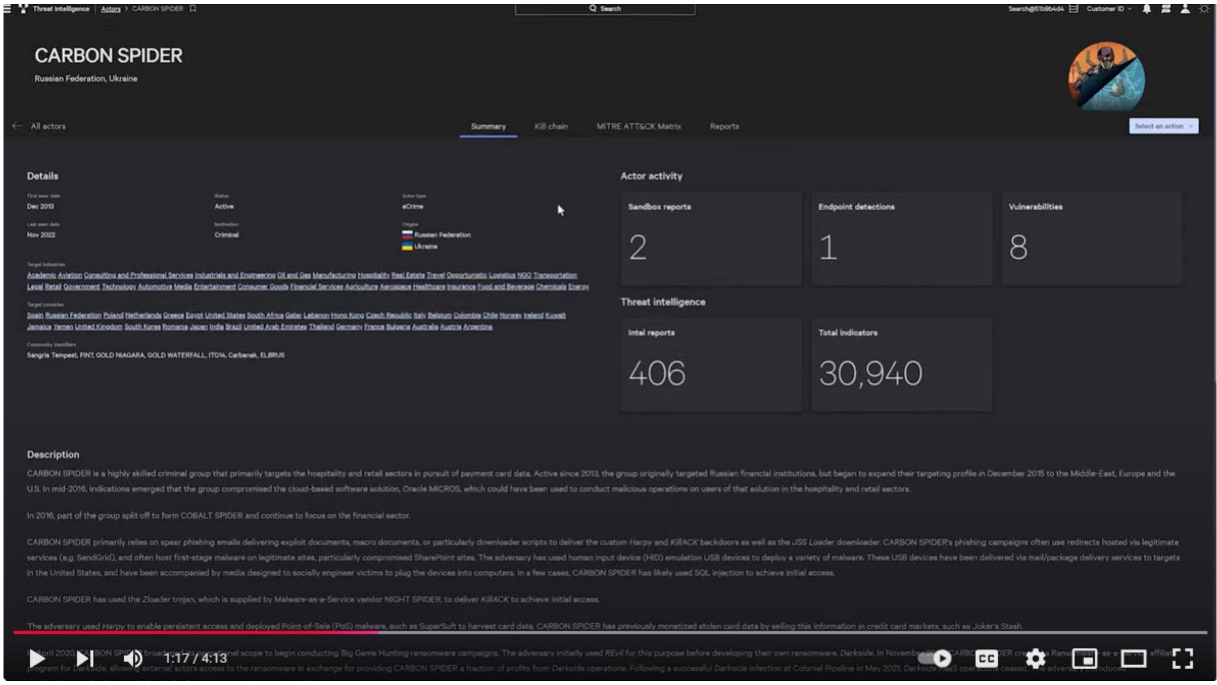
Actors BITWISE SPIDER — See more about BITWISE SPIDER
Last active: Sep 2023 | Status: Active | Origin: Unknown
Intel reports: 241 | Target industries: 42 | Target countries: 93
Actor type: eCrime | Motivation: Criminal
Community identifiers: LockBit, LockBitSupp, StealBit
Seen in your environment: 1 0 0

Actors BRAIN SPIDER — See more about BRAIN SPIDER
Last active: Sep 2023 | Status: Active | Origin: Russian Federation, Eastern Europe
Intel reports: 14 | Target industries: 10 | Target countries: 5
Actor type: eCrime | Motivation: Criminal
Community identifiers: RAID, Signature, brain, bigboss, reverse6net, SBIRD, bigrichy, FASTPRISONER, exp3rt, RedTeam, BOSS
Seen in your environment: 1 0 0

Actors CARBON SPIDER — See more about CARBON SPIDER
Last active: Nov 2022 | Status: Active | Origin: Russian Federation, Ukraine
Intel reports: 403 | Target industries: 29 | Target countries: 38
Actor type: eCrime | Motivation: Criminal
Community identifiers: GOLD WATERFALL, ITG14, Carbanak, ELBRUS, Sangria Tempest, FIN7, GOLD NIAGARA
Seen in your environment: 8 1 2

Actors GRACEFUL SPIDER — See more about GRACEFUL SPIDER
Last active: Aug 2023 | Status: Active | Origin: Russian Federation, Eastern Europe
Intel reports: 208 | Target industries: 35 | Target countries: 35
Actor type: eCrime | Motivation: Criminal
Community identifiers: FIN11, Clop

Actors NIGHT SPIDER — See more about NIGHT SPIDER
Last active: Mar 2022 | Status: Inactive | Origin: Unknown
Intel reports: 20 | Target industries: 1 | Target countries: 0
Actor type: eCrime | Motivation: Criminal
Community identifiers: Zloader, Silent Night, DELoader, Terdot

[42]

Threat intelligence | Actors > CARBON SPIDER

CARBON SPIDER
Russian Federation, Ukraine

Details

First seen date: Dec 2013 | Status: Active | Actor type: eCrime
Last seen date: Nov 2022 | Motivation: Criminal | Origins: Russian Federation, Ukraine

Target industries: Academic Aviation Consulting and Professional Services Industrials and Engineering Oil and Gas Manufacturing Hospitality Real Estate Travel Opportunistic Logistics NGO Transportation Legal Retail Government Technology Automotive Media Entertainment Consumer Goods Financial Services Agriculture Aerospace Healthcare Insurance Food and Beverage Chemicals Energy

Target countries: Spain Russian Federation Poland Netherlands Greece Egypt United States South Africa Qatar Lebanon Hong Kong Czech Republic Italy Belgium Colombia Chile Norway Ireland Kuwait Jamaica Yemen United Kingdom South Korea Romania Japan India Brazil United Arab Emirates Thailand Germany France Bulgaria Australia Austria Argentina

Community identifiers: Sangria Tempest, FIN7, GOLD NIAGARA, GOLD WATERFALL, ITG14, Carbanak, ELBRUS

Actor activity

Sandbox reports: 2 | Endpoint detections: 1 | Vulnerabilities: 8

Threat intelligence

Intel reports: 406 | Total indicators: 30,940

Description

CARBON SPIDER is a highly skilled criminal group that primarily targets the hospitality and retail sectors in pursuit of payment card data. Active since 2013, the group originally targeted Russian financial institutions, but began to expand their targeting profile in December 2015 to the Middle-East, Europe and the U.S. In mid-2016, indications emerged that the group compromised the cloud-based software solution, Oracle MICROS, which could have been used to conduct malicious operations on users of that solution in the hospitality and retail sectors.

In 2016, part of the group split off to form COBALT SPIDER and continue to focus on the financial sector.

CARBON SPIDER primarily relies on spear phishing emails delivering exploit documents, macro documents, or particularly downloader scripts to deliver the custom *Harpy* and *KillACK* backdoors as well as the *JSS Loader* downloader. CARBON SPIDER's phishing campaigns often use redirects hosted via legitimate services (e.g. SendGrid), and often host first-stage malware on legitimate sites, particularly compromised SharePoint sites. The adversary has used human input device (HID) emulation USB devices to deploy a variety of malware. These USB devices have been delivered via mail/package delivery services to targets in the United States, and have been accompanied by media designed to socially engineer victims to plug the devices into computers. In a few cases, CARBON SPIDER has likely used SQL injection to achieve initial access.

CARBON SPIDER has used the *Zloader* trojan, which is supplied by Malware-as-a-Service vendor NIGHT SPIDER, to deliver *KillACK* to achieve initial access.

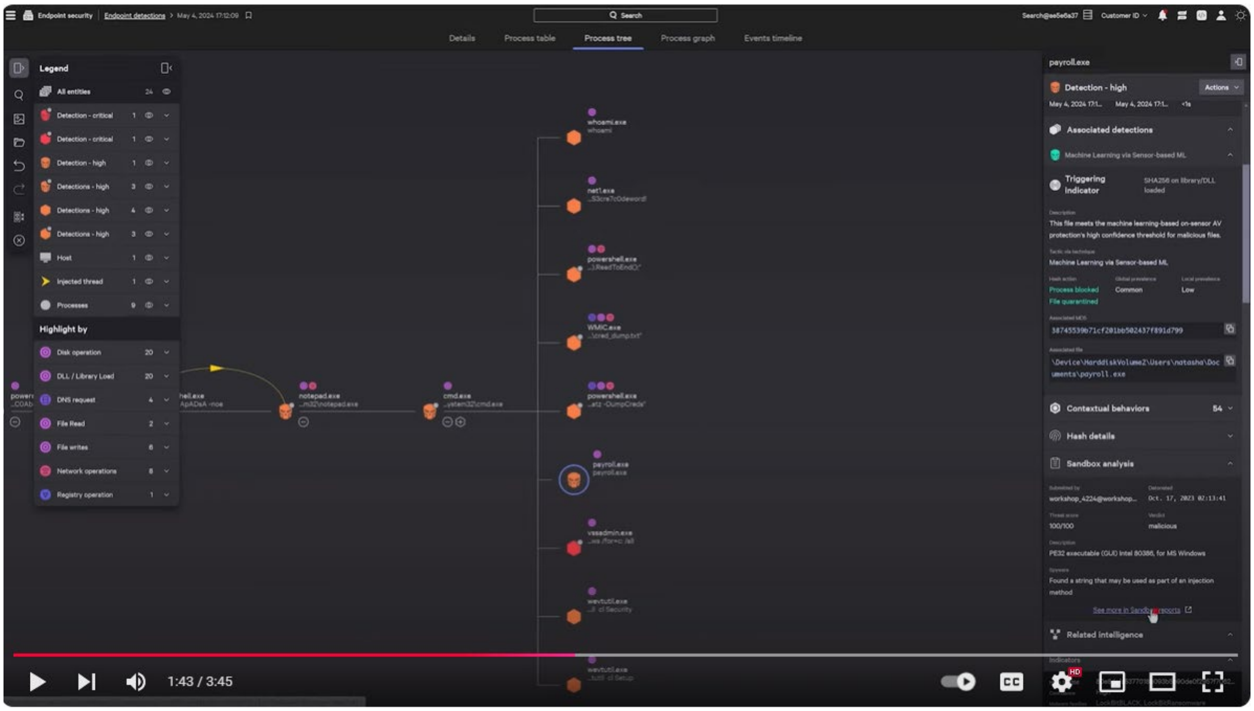
The adversary used *Harpy* to enable persistent access and deployed Point-of-Sale (PoS) malware, such as SuperSoft to harvest card data. CARBON SPIDER has previously monetized stolen card data by selling this information in credit card markets, such as Joker's Stash.

April 2020, BON SP broad onal scope to begin conducting Big Game Hunting ransomware campaigns. The adversary initially used *REvil* for this purpose before developing their own ransomware, *Darkside*. In Novemb CARBO ER cr Ransom as-a affiliate program for *Darkside*, allowing external actors access to the ransomware in exchange for providing CARBON SPIDER a fraction of profits from *Darkside* operations. Following a successful *Darkside* infection at Colonial Pipeline in May 2021, Darkside RaaS operations ceased. adversary introduced

74. In another example, a malicious file ("payroll.exe" associated with Carbon Spider is detected. The Falcon Platform "immediately alert[s] [customers] if Carbon Spider is active . . . even if they're using never-before-seen techniques. With full attribution, [CrowdStrike customers]

[42] https://www.youtube.com/watch?v=RrKQN8x2Ldc.

are made aware of all relevant behaviors and vulnerabilities being targeted across [their] environment directly from detections." In this example, a Falcon Platform user investigating "payroll.exe" identifies 1,591 "Vulnerabilities" associated with the associated actor (Carbon Spider) in the exemplary computer environment.



payroll.exe

Detection - high Actions

May 4, 2024 17:1... May 4, 2024 17:1... <1s

Associated detections

Machine Learning via Sensor-based ML

Triggering Indicator: SHA256 on library/DLL loaded

Description: This file meets the machine learning-based on-sensor AV protection's high confidence threshold for malicious files.

Tactic via technique: Machine Learning via Sensor-based ML

Hash action: Process blocked, File quarantined | Global prevalence: Common | Local prevalence: Low

Associated MD5: 38745539b71cf201bb502437f891d799

Associated file: \Device\HarddiskVolume2\Users\natasha\Documents\payroll.exe

Contextual behaviors 54

Hash details

Sandbox analysis

Submitted by: workshop_4224@workshop... | Detonated: Oct. 17, 2023 02:13:41

Threat score: 100/100 | Verdict: malicious

Description: PE32 executable (GUI) Intel 80386, for MS Windows

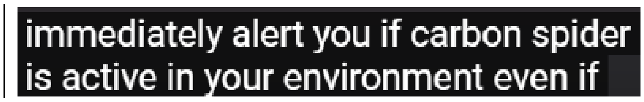
Signature: Found a string that may be used as part of an injection method

See more in Sandbox reports

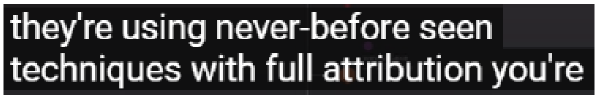
Related intelligence

Indicators

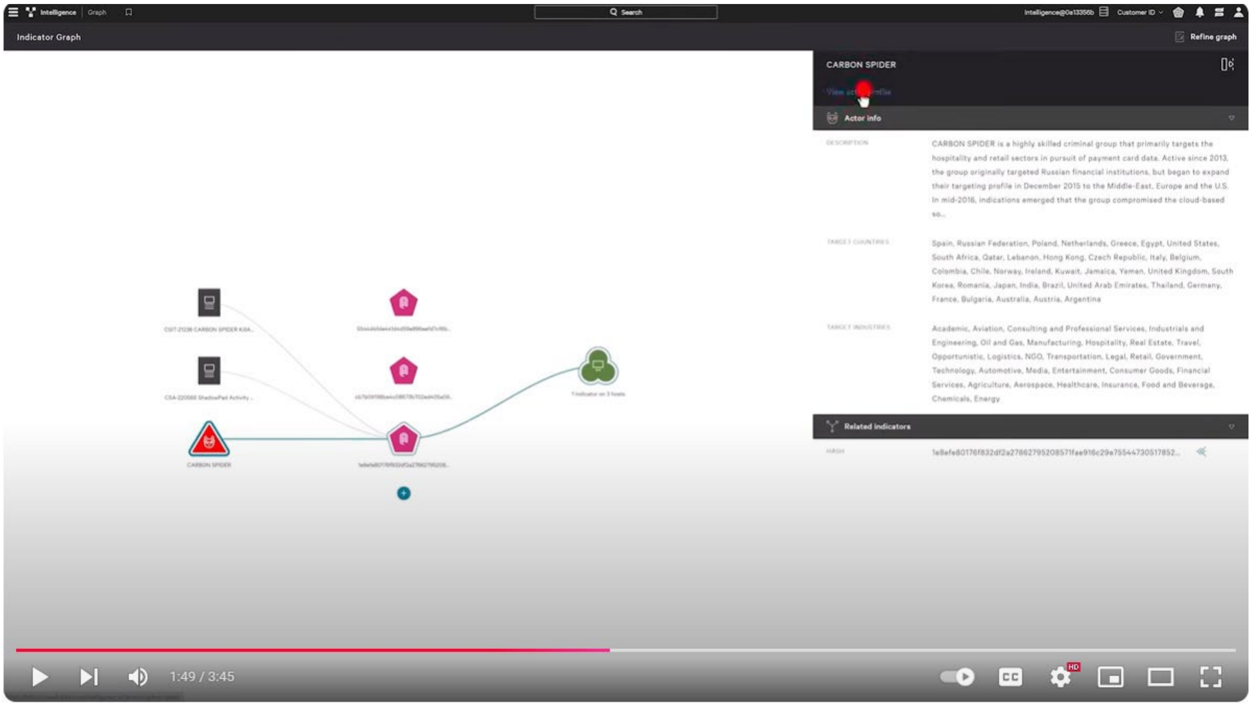
Malware families: LockBitBLACK, LockBitRansomware



immediately alert you if carbon spider
is active in your environment even if



they're using never-before seen
techniques with full attribution you're



CARBON SPIDER

View actor profile

Actor info

DESCRIPTION: CARBON SPIDER is a highly skilled criminal group that primarily targets the hospitality and retail sectors in pursuit of payment card data. Active since 2013, the group originally targeted Russian financial institutions, but began to expand their targeting profile in December 2015 to the Middle-East, Europe and the U.S. In mid-2016, indications emerged that the group compromised the cloud-based so...

TARGET COUNTRIES: Spain, Russian Federation, Poland, Netherlands, Greece, Egypt, United States, South Africa, Qatar, Lebanon, Hong Kong, Czech Republic, Italy, Belgium, Colombia, Chile, Norway, Ireland, Kuwait, Jamaica, Yemen, United Kingdom, South Korea, Romania, Japan, India, Brazil, United Arab Emirates, Thailand, Germany, France, Bulgaria, Australia, Austria, Argentina

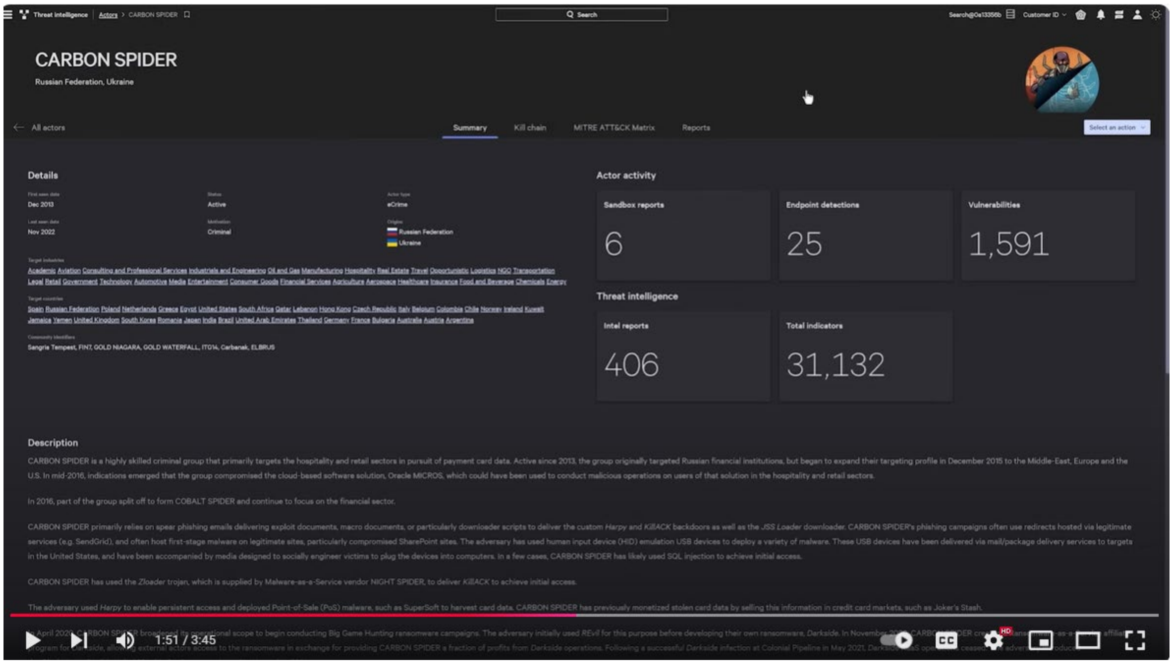
TARGET INDUSTRIES: Academic, Aviation, Consulting and Professional Services, Industrials and Engineering, Oil and Gas, Manufacturing, Hospitality, Real Estate, Travel, Opportunistic, Logistics, NGO, Transportation, Legal, Retail, Government, Technology, Automotive, Media, Entertainment, Consumer Goods, Financial Services, Agriculture, Aerospace, Healthcare, Insurance, Food and Beverage, Chemicals, Energy

Related indicators

HASH: 1e8efe80176f832df2a27862795208571fae916c29e75544730517852...

made aware of all relevant behavior and vulnerabilities being targeted across

your environment directly from detections your team can quickly



CARBON SPIDER

Russian Federation, Ukraine

Details

First seen date: Dec 2013

Status: Active

Actor type: eCrime

Last seen date: Nov 2022

Motivation: Criminal

Origins: Russian Federation, Ukraine

Target industries: Academic Aviation Consulting and Professional Services Industrials and Engineering Oil and Gas Manufacturing Hospitality Real Estate Travel Opportunistic Logistics NGO Transportation Legal Retail Government Technology Automotive Media Entertainment Consumer Goods Financial Services Agriculture Aerospace Healthcare Insurance Food and Beverage Chemicals Energy

Target countries: Spain Russian Federation Poland Netherlands Greece Egypt United States South Africa Qatar Lebanon Hong Kong Czech Republic Italy Belgium Colombia Chile Norway Ireland Kuwait Jamaica Yemen United Kingdom South Korea Romania Japan India Brazil United Arab Emirates Thailand Germany France Bulgaria Australia Austria Argentina

Community identifiers: Sangria Tempest, FIN7, GOLD NIAGARA, GOLD WATERFALL, ITG14, Carbanak, ELBRUS

Actor activity

Sandbox reports	Endpoint detections	Vulnerabilities
6	25	1,591

Threat intelligence

Intel reports	Total indicators
406	31,132

Description

CARBON SPIDER is a highly skilled criminal group that primarily targets the hospitality and retail sectors in pursuit of payment card data. Active since 2013, the group originally targeted Russian financial institutions, but began to expand their targeting profile in December 2015 to the Middle-East, Europe and the U.S. In mid-2016, indications emerged that the group compromised the cloud-based software solution, Oracle MICROS, which could have been used to conduct malicious operations on users of that solution in the hospitality and retail sectors.

In 2016, part of the group split off to form COBALT SPIDER and continue to focus on the financial sector.

CARBON SPIDER primarily relies on spear phishing emails delivering exploit documents, macro documents, or particularly downloader scripts to deliver the custom *Harpy* and *KillACK* backdoors as well as the *JSS Loader* downloader. CARBON SPIDER's phishing campaigns often use redirects hosted via legitimate services (e.g. SendGrid), and often host first-stage malware on legitimate sites, particularly compromised SharePoint sites. The adversary has used human input device (HID) emulation USB devices to deploy a variety of malware. These USB devices have been delivered via mail/package delivery services to targets in the United States, and have been accompanied by media designed to socially engineer victims to plug the devices into computers. In a few cases, CARBON SPIDER has likely used SQL injection to achieve initial access.

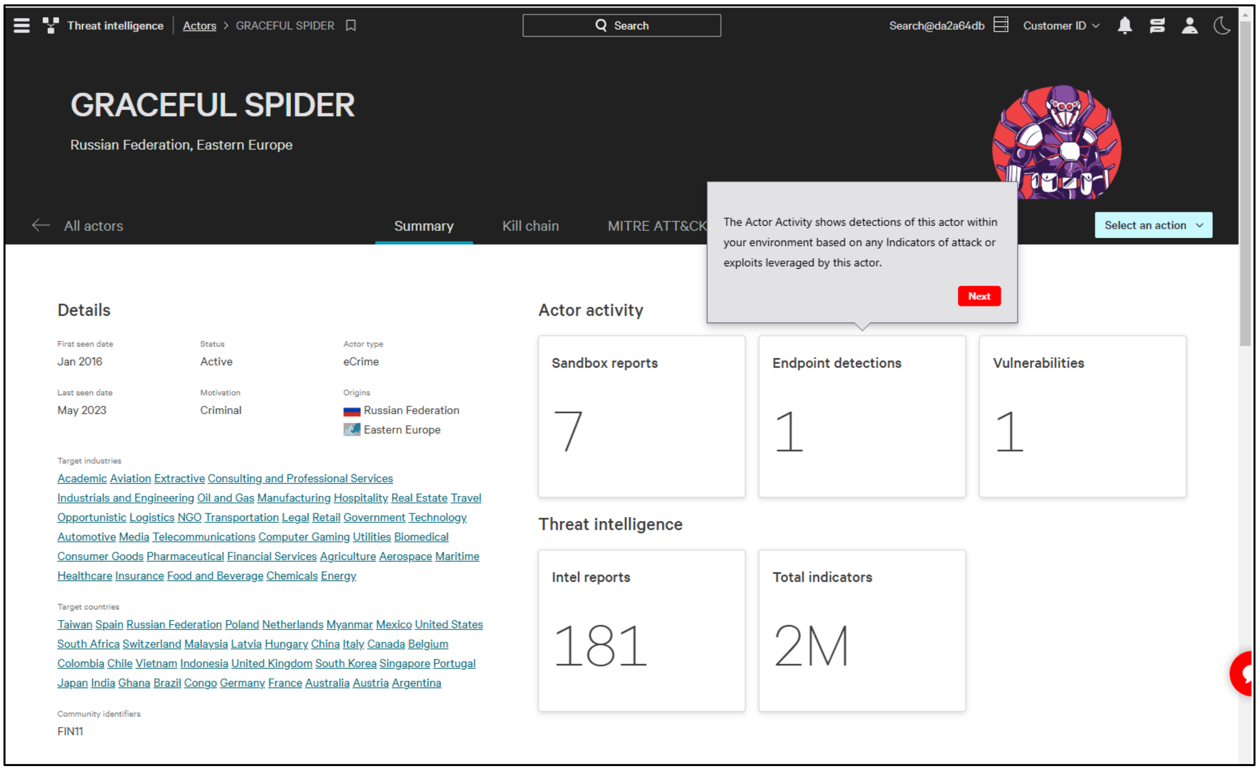
CARBON SPIDER has used the *Zloader* trojan, which is supplied by Malware-as-a-Service vendor NIGHT SPIDER, to deliver *KillACK* to achieve initial access.

The adversary used *Harpy* to enable persistent access and deployed Point-of-Sale (PoS) malware, such as SuperSoft to harvest card data. CARBON SPIDER has previously monetized stolen card data by selling this information in credit card markets, such as Joker's Stash.

[43]

[43] https://www.youtube.com/watch?v=nUS_x-VatAo.

75. In a related example, a demo of Falcon Adversary Intelligence demonstrates a threat intelligence actor page for criminal group "GRACEFUL SPIDER" and an exemplary 1 "Endpoint detections" and 1 "Vulnerabilities" for an exemplary computer system. Indeed, the "Actor Activity shows detections of this actor within [a customer's computer] environment based on any Indicators of attack or exploits leveraged by this actor" (e.g., exploits by Graceful Spider) (analyzing the application of the set of exploits on the computer system to detect a particular vulnerability of the computer system). Related indicators (e.g., indicators of compromise, indicators of attack) can be further accessed "by clicking on the number in the Total indicators box" (in this example, "2M"), which brings a Falcon Platform customer to the "Falcon Intelligence Indicator Page."



GRACEFUL SPIDER

Russian Federation, Eastern Europe

The Actor Activity shows detections of this actor within your environment based on any Indicators of attack or exploits leveraged by this actor.

Details

First seen date: Jan 2016

Status: Active

Actor type: eCrime

Last seen date: May 2023

Motivation: Criminal

Origins: Russian Federation, Eastern Europe

Target industries

Academic Aviation Extractive Consulting and Professional Services Industrials and Engineering Oil and Gas Manufacturing Hospitality Real Estate Travel Opportunistic Logistics NGO Transportation Legal Retail Government Technology Automotive Media Telecommunications Computer Gaming Utilities Biomedical Consumer Goods Pharmaceutical Financial Services Agriculture Aerospace Maritime Healthcare Insurance Food and Beverage Chemicals Energy

Target countries

Taiwan Spain Russian Federation Poland Netherlands Myanmar Mexico United States South Africa Switzerland Malaysia Latvia Hungary China Italy Canada Belgium Colombia Chile Vietnam Indonesia United Kingdom South Korea Singapore Portugal Japan India Ghana Brazil Congo Germany France Australia Austria Argentina

Community identifiers

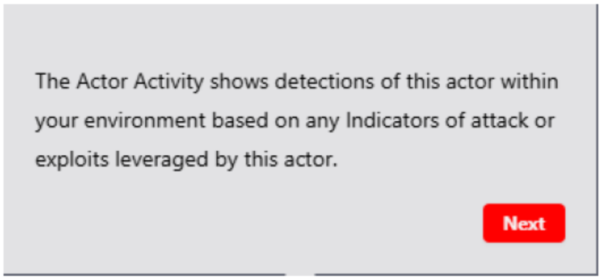
FIN11

Actor activity

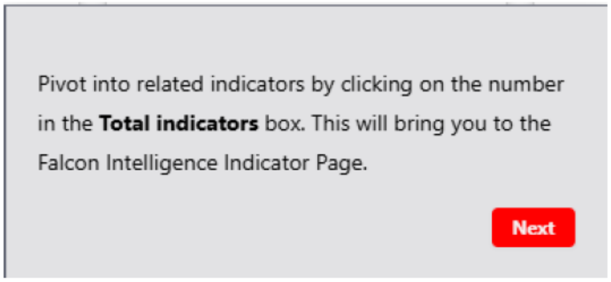
Sandbox reports	Endpoint detections	Vulnerabilities
7	1	1

Threat intelligence

Intel reports	Total indicators
181	2M



The Actor Activity shows detections of this actor within your environment based on any Indicators of attack or exploits leveraged by this actor.



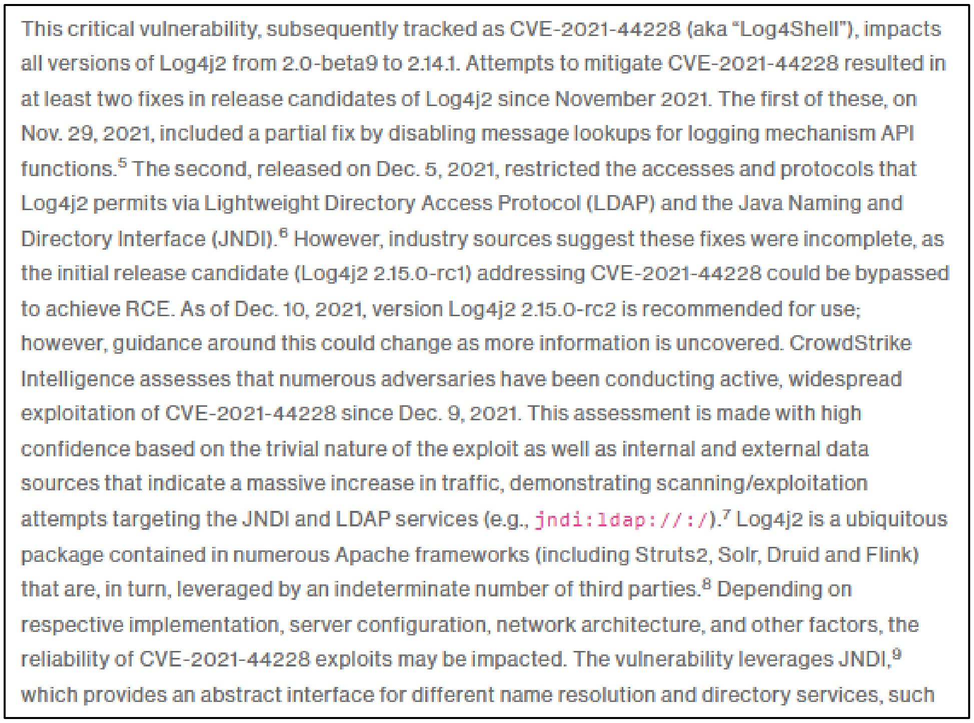
Pivot into related indicators by clicking on the number in the **Total indicators** box. This will bring you to the Falcon Intelligence Indicator Page.

[44]

76. Additional examples below demonstrate how CrowdStrike has implemented exploit and vulnerability analysis within the Falcon Platform, including conducts detailed examinations regarding how exploits are applied to computer systems and identifications of specific vulnerabilities that could be exploited by adversaries from such exploits.

77. The CrowdStrike indicates that their systems and services perform actions that involve analyzing the application of a set of exploits on computer systems to detect particular vulnerabilities within those systems. Specifically, CrowdStrike conducts detailed examinations of how exploits are applied to systems and identifies specific vulnerabilities that could be exploited by adversaries. For example, "CrowdStrike Intelligence assesses that numerous adversaries have . . . exploit[ed] [] CVE-2021-44228 [(Log4Shell, impacting "all versions of Log4j2 from 2.0-beta9 to 2.14.1")] since Dec. 9, 2021."

[44] https://www.crowdstrike.com/en-us/interactive-demos/threat-intel/demo/.



This critical vulnerability, subsequently tracked as CVE-2021-44228 (aka "Log4Shell"), impacts all versions of Log4j2 from 2.0-beta9 to 2.14.1. Attempts to mitigate CVE-2021-44228 resulted in at least two fixes in release candidates of Log4j2 since November 2021. The first of these, on Nov. 29, 2021, included a partial fix by disabling message lookups for logging mechanism API functions.[5] The second, released on Dec. 5, 2021, restricted the accesses and protocols that Log4j2 permits via Lightweight Directory Access Protocol (LDAP) and the Java Naming and Directory Interface (JNDI).[6] However, industry sources suggest these fixes were incomplete, as the initial release candidate (Log4j2 2.15.0-rc1) addressing CVE-2021-44228 could be bypassed to achieve RCE. As of Dec. 10, 2021, version Log4j2 2.15.0-rc2 is recommended for use; however, guidance around this could change as more information is uncovered. CrowdStrike Intelligence assesses that numerous adversaries have been conducting active, widespread exploitation of CVE-2021-44228 since Dec. 9, 2021. This assessment is made with high confidence based on the trivial nature of the exploit as well as internal and external data sources that indicate a massive increase in traffic, demonstrating scanning/exploitation attempts targeting the JNDI and LDAP services (e.g., `jndi:ldap://:/`).[7] Log4j2 is a ubiquitous package contained in numerous Apache frameworks (including Struts2, Solr, Druid and Flink) that are, in turn, leveraged by an indeterminate number of third parties.[8] Depending on respective implementation, server configuration, network architecture, and other factors, the reliability of CVE-2021-44228 exploits may be impacted. The vulnerability leverages JNDI,[9] which provides an abstract interface for different name resolution and directory services, such [45]

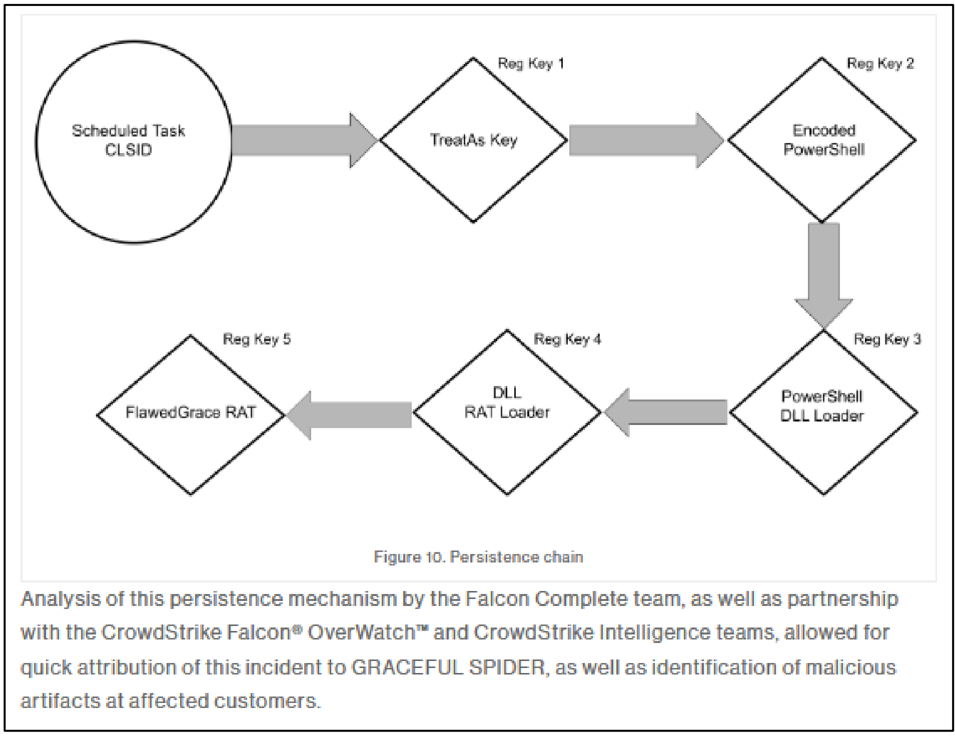


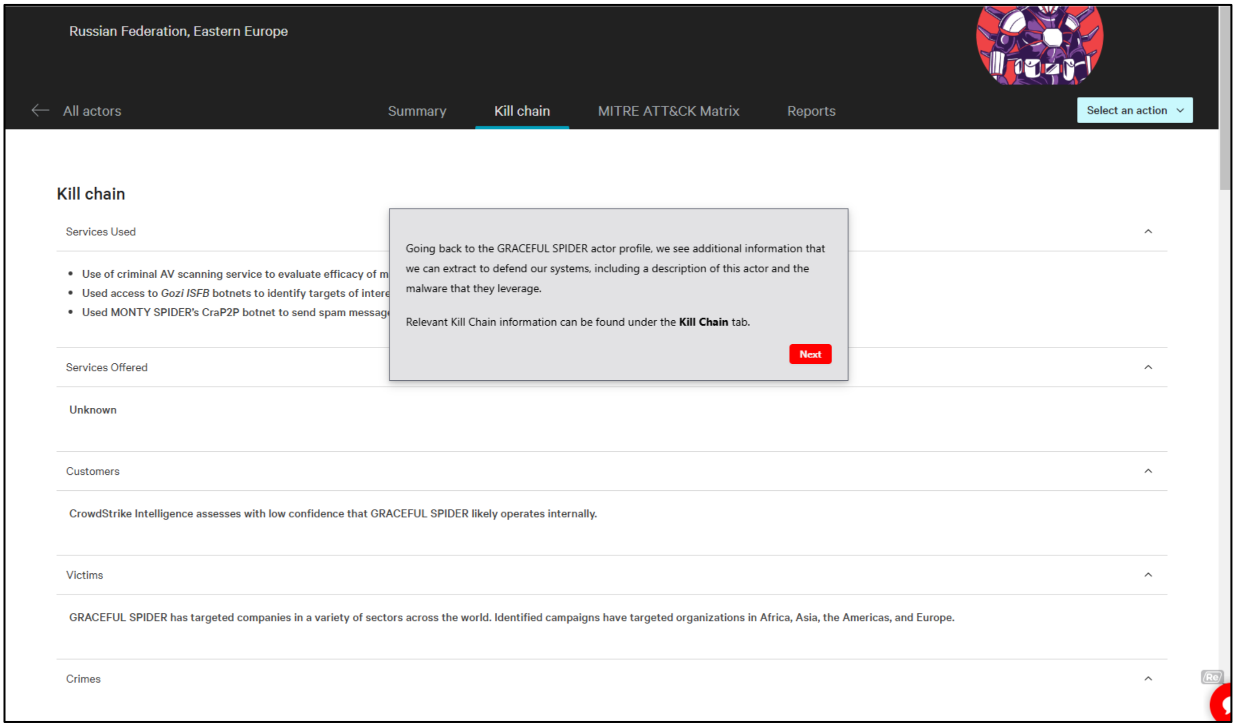
Figure 10. Persistence chain

Analysis of this persistence mechanism by the Falcon Complete team, as well as partnership with the CrowdStrike Falcon® OverWatch™ and CrowdStrike Intelligence teams, allowed for quick attribution of this incident to GRACEFUL SPIDER, as well as identification of malicious artifacts at affected customers. [46]

[45] https://www.crowdstrike.com/en-us/blog/log4j2-vulnerability-analysis-and-mitigation-recommendations.

[46] https://www.crowdstrike.com/en-us/blog/how-falcon-complete-stopped-a-solarwinds-serv-u-exploit-campaign/.

78. The Falcon Platform performs a method that includes *altering a configuration of the computer system in response to the analysis of the application of the set of exploits to reduce potential damage of a cyberattack*. For instance, using the Falcon Adversary Intelligence module, the "Kill chain" tab provides information about an adversary actor (in this example, Graceful Spider) such as "malware that they leverage." Also included in the Kill chain tab is an "Exploitation" section that "contains all the CVE's [Common Vulnerabilities and Exposures] that [an] actor is known to leverage in their attacks" (analysis of the application of the set of exploits). In this example, the Exploitation section for Graceful Spider identifies "CVE-2021-35211, CVE-2020-0787" and a link to "1 vulnerabilities found." This vulnerability "can be sent to the vulnerability management team to prioritize patching."



Kill chain

Services Used

- Use of criminal AV scanning service to evaluate efficacy of m
- Used access to *Gozi ISFB* botnets to identify targets of intere
- Used MONTY SPIDER's CraP2P botnet to send spam messag

Going back to the GRACEFUL SPIDER actor profile, we see additional information that we can extract to defend our systems, including a description of this actor and the malware that they leverage.

Relevant Kill Chain information can be found under the **Kill Chain** tab.

Services Offered

Unknown

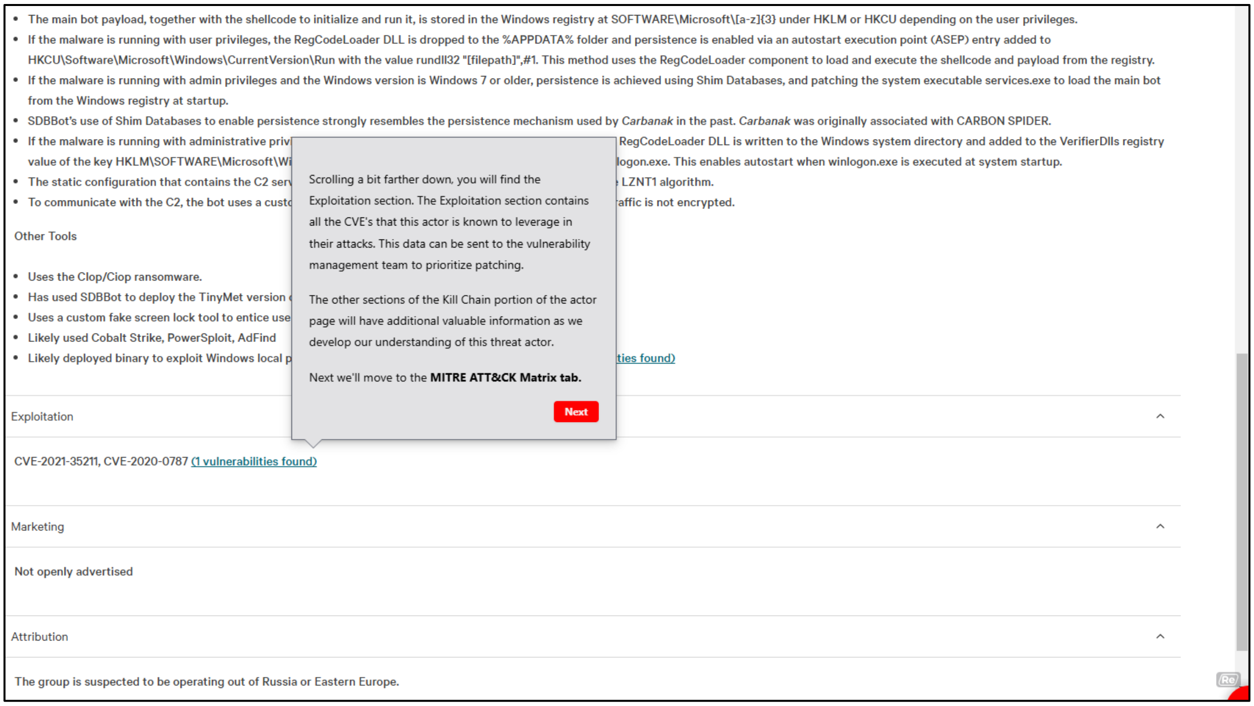
Customers

CrowdStrike Intelligence assesses with low confidence that GRACEFUL SPIDER likely operates internally.

Victims

GRACEFUL SPIDER has targeted companies in a variety of sectors across the world. Identified campaigns have targeted organizations in Africa, Asia, the Americas, and Europe.

Crimes



- The main bot payload, together with the shellcode to initialize and run it, is stored in the Windows registry at SOFTWARE\Microsoft\[a-z]{3} under HKLM or HKCU depending on the user privileges.
- If the malware is running with user privileges, the RegCodeLoader DLL is dropped to the %APPDATA% folder and persistence is enabled via an autostart execution point (ASEP) entry added to HKCU\Software\Microsoft\Windows\CurrentVersion\Run with the value rundll32 "[filepath]",#1. This method uses the RegCodeLoader component to load and execute the shellcode and payload from the registry.
- If the malware is running with admin privileges and the Windows version is Windows 7 or older, persistence is achieved using Shim Databases, and patching the system executable services.exe to load the main bot from the Windows registry at startup.
- SDBBot's use of Shim Databases to enable persistence strongly resembles the persistence mechanism used by *Carbanak* in the past. *Carbanak* was originally associated with CARBON SPIDER.
- If the malware is running with administrative privi RegCodeLoader DLL is written to the Windows system directory and added to the VerifierDlls registry value of the key HKLM\SOFTWARE\Microsoft\Wi logon.exe. This enables autostart when winlogon.exe is executed at system startup.
- The static configuration that contains the C2 serv LZNT1 algorithm.
- To communicate with the C2, the bot uses a custo affic is not encrypted.

Other Tools

- Uses the Clop/Ciop ransomware.
- Has used SDBBot to deploy the TinyMet version
- Uses a custom fake screen lock tool to entice use
- Likely used Cobalt Strike, PowerSploit, AdFind
- Likely deployed binary to exploit Windows local p ties found)

Scrolling a bit farther down, you will find the Exploitation section. The Exploitation section contains all the CVE's that this actor is known to leverage in their attacks. This data can be sent to the vulnerability management team to prioritize patching.

The other sections of the Kill Chain portion of the actor page will have additional valuable information as we develop our understanding of this threat actor.

Next we'll move to the **MITRE ATT&CK Matrix tab.**

Exploitation

CVE-2021-35211, CVE-2020-0787 (1 vulnerabilities found)

Marketing

Not openly advertised

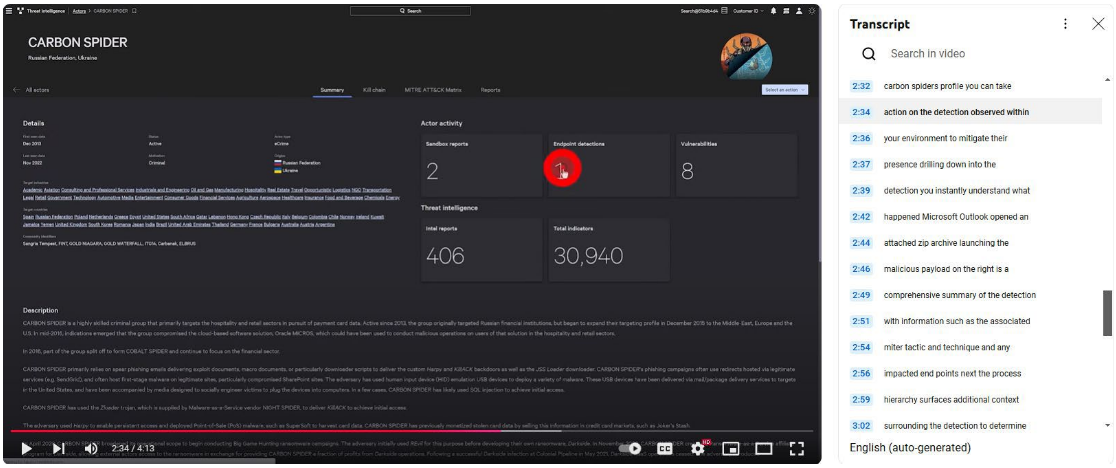
Attribution

The group is suspected to be operating out of Russia or Eastern Europe.

[47]

79. In another Falcon Adversary Intelligence example, customers can click on the "Endpoint detections" box to "take action on the detection observed within [their] environment to mitigate [an adversary's] presence" (analysis of the application of the set of exploits). In this example, a detection triggered by "gspider.exe" from "Microsoft Outlook open[ing] an attached zip archive launching the malicious payload." In this example, the "process is immediately blocked in the file quarantined by the [Falcon] platform. Falcon Adversary Intelligence automatically detonates quarantined files in a secure environment to understand the severity score and risk" and the resulting "sandbox report" can "surface hidden IOCs [indicators of compromise] that can be leveraged to prevent future attacks."

[47] https://www.crowdstrike.com/en-us/interactive-demos/threat-intel/demo/.



Threat intelligence | Actors > CARBON SPIDER

CARBON SPIDER
Russian Federation, Ukraine

All actors | Summary | Kill chain | MITRE ATT&CK Matrix | Reports | Select an action

Details

First seen date: Dec 2013 | Status: Active | Actor type: eCrime
Last seen date: Nov 2022 | Motivation: Criminal | Origins: Russian Federation, Ukraine

Target industries: Academic Aviation Consulting and Professional Services Industrials and Engineering Oil and Gas Manufacturing Hospitality Real Estate Travel Opportunistic Logistics NGO Transportation Legal Retail Government Technology Automotive Media Entertainment Consumer Goods Financial Services Agriculture Aerospace Healthcare Insurance Food and Beverage Chemicals Energy

Target countries: Spain Russian Federation Poland Netherlands Greece Egypt United States South Africa Qatar Lebanon Hong Kong Czech Republic Italy Belgium Colombia Chile Norway Ireland Kuwait Jamaica Yemen United Kingdom South Korea Romania Japan India Brazil United Arab Emirates Thailand Germany France Bulgaria Australia Austria Argentina

Community identifiers: Sangria Tempest, FIN7, GOLD NIAGARA, GOLD WATERFALL, ITG14, Carbanak, ELBRUS

Actor activity

Sandbox reports	Endpoint detections	Vulnerabilities
2	1	8

Threat intelligence

Intel reports	Total indicators
406	30,940

Description

CARBON SPIDER is a highly skilled criminal group that primarily targets the hospitality and retail sectors in pursuit of payment card data. Active since 2013, the group originally targeted Russian financial institutions, but began to expand their targeting profile in December 2015 to the Middle-East, Europe and the U.S. In mid-2016, indications emerged that the group compromised the cloud-based software solution, Oracle MICROS, which could have been used to conduct malicious operations on users of that solution in the hospitality and retail sectors.

In 2016, part of the group split off to form COBALT SPIDER and continue to focus on the financial sector.

CARBON SPIDER primarily relies on spear phishing emails delivering exploit documents, macro documents, or particularly downloader scripts to deliver the custom *Harpy* and *KillACK* backdoors as well as the *JSS Loader* downloader. CARBON SPIDER's phishing campaigns often use redirects hosted via legitimate services (e.g. SendGrid), and often host first-stage malware on legitimate sites, particularly compromised SharePoint sites. The adversary has used human input device (HID) emulation USB devices to deploy a variety of malware. These USB devices have been delivered via mail/package delivery services to targets in the United States, and have been accompanied by media designed to socially engineer victims to plug the devices into computers. In a few cases, CARBON SPIDER has likely used SQL injection to achieve initial access.

CARBON SPIDER has used the *Zloader* trojan, which is supplied by Malware-as-a-Service vendor NIGHT SPIDER, to deliver *KillACK* to achieve initial access.

The adversary used *Harpy* to enable persistent access and deployed Point-of-Sale (PoS) malware, such as SuperSoft to harvest card data. CARBON SPIDER has previously monetized stolen card data by selling this information in credit card markets, such as Joker's Stash.

In April 2020, CARBON SPIDER broadened its operational scope to begin conducting Big Game Hunting ransomware campaigns. The adversary initially used *REvil* for this purpose before developing their own ransomware, *Darkside*. In November [illegible] CARBON SPIDER [illegible] affiliate program for Darkside, allowing external actors access to the ransomware in exchange for providing CARBON SPIDER a fraction of profits from Darkside operations. Following a successful Darkside infection at Colonial Pipeline in May 2021, Darkside [illegible]

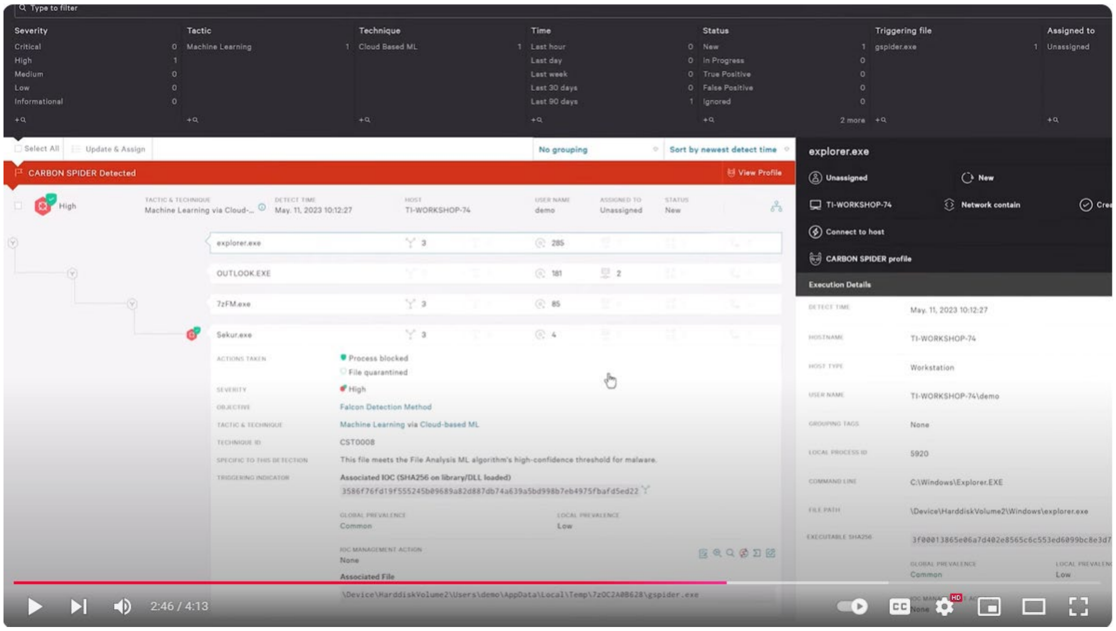
2:34 / 4:13

Transcript

Search in video

2:32 carbon spiders profile you can take
2:34 action on the detection observed within
2:36 your environment to mitigate their
2:37 presence drilling down into the
2:39 detection you instantly understand what
2:42 happened Microsoft Outlook opened an
2:44 attached zip archive launching the
2:46 malicious payload on the right is a
2:49 comprehensive summary of the detection
2:51 with information such as the associated
2:54 miter tactic and technique and any
2:56 impacted end points next the process
2:59 hierarchy surfaces additional context
3:02 surrounding the detection to determine

English (auto-generated)



Type to filter

Severity		Tactic		Technique		Time		Status		Triggering file		Assigned to	
Critical	0	Machine Learning	1	Cloud Based ML	1	Last hour	0	New	1	gspider.exe	1	Unassigned	
High	1					Last day	0	In Progress	0				
Medium	0					Last week	0	True Positive	0				
Low	0					Last 30 days	0	False Positive	0				
Informational	0					Last 90 days	1	Ignored	0				
									2 more				

Select All | Update & Assign | No grouping | Sort by newest detect time

CARBON SPIDER Detected | View Profile

High | Tactic & technique: Machine Learning via Cloud-... | Detect time: May. 11, 2023 10:12:27 | Host: TI-WORKSHOP-74 | User name: demo | Assigned to: Unassigned | Status: New

explorer.exe	3	285	
OUTLOOK.EXE		181	2
7zFM.exe	3	85	
Sekur.exe	3	4	

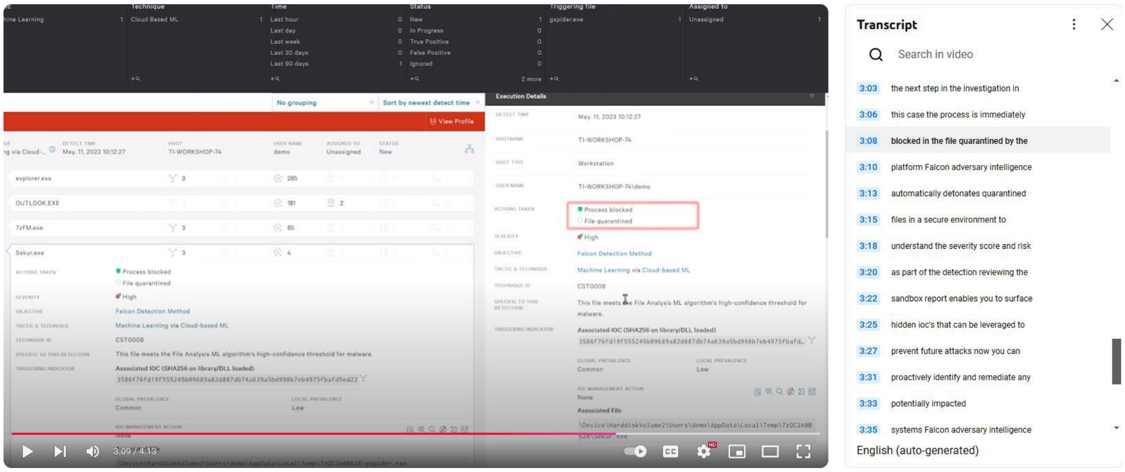
ACTIONS TAKEN: Process blocked; File quarantined
SEVERITY: High
OBJECTIVE: Falcon Detection Method
TACTIC & TECHNIQUE: Machine Learning via Cloud-based ML
TECHNIQUE ID: CST0008
SPECIFIC TO THIS DETECTION: This file meets the File Analysis ML algorithm's high-confidence threshold for malware.
TRIGGERING INDICATOR: Associated IOC (SHA256 on library/DLL loaded)
3586f76fd19f555245b09689a82d887db74a639a5bd998b7eb4975fbafd5ed22
GLOBAL PREVALENCE: Common | LOCAL PREVALENCE: Low
IOC MANAGEMENT ACTION: None
Associated File
\Device\HarddiskVolume2\Users\demo\AppData\Local\Temp\7zOC2A0B628\gspider.exe

explorer.exe
Unassigned | New
TI-WORKSHOP-74 | Network contain | Cre
Connect to host
CARBON SPIDER profile

Execution Details

DETECT TIME: May. 11, 2023 10:12:27
HOSTNAME: TI-WORKSHOP-74
HOST TYPE: Workstation
USER NAME: TI-WORKSHOP-74\demo
GROUPING TAGS: None
LOCAL PROCESS ID: 5920
COMMAND LINE: C:\Windows\Explorer.EXE
FILE PATH: \Device\HarddiskVolume2\Windows\explorer.exe
EXECUTABLE SHA256: 3f00013865e06a7d402e8565c6c553ed6099bc8e3d7
GLOBAL PREVALENCE: Common | LOCAL PREVALENCE: Low
IOC MANAGEMENT ACTION: None

2:46 / 4:13



Execution Details

DETECT TIME: May. 11, 2023 10:12:27
HOSTNAME: TI-WORKSHOP-74
HOST TYPE: Workstation
USER NAME: TI-WORKSHOP-74\demo
ACTIONS TAKEN: Process blocked; File quarantined
SEVERITY: High
OBJECTIVE: Falcon Detection Method
TACTIC & TECHNIQUE: Machine Learning via Cloud-based ML
TECHNIQUE ID: CST0008
SPECIFIC TO THIS DETECTION: This file meets the File Analysis ML algorithm's high-confidence threshold for malware.
TRIGGERING INDICATOR: Associated IOC (SHA256 on library/DLL loaded)
3586f76fd19f555245b09689a82d887db74a639a5bd998b7eb4975fbafd...
GLOBAL PREVALENCE: Common | LOCAL PREVALENCE: Low
IOC MANAGEMENT ACTION: None
Associated File
\Device\HarddiskVolume2\Users\demo\AppData\Local\Temp\7zOC2A0B628\gspider.exe

3:09 / 4:13

Transcript

Search in video

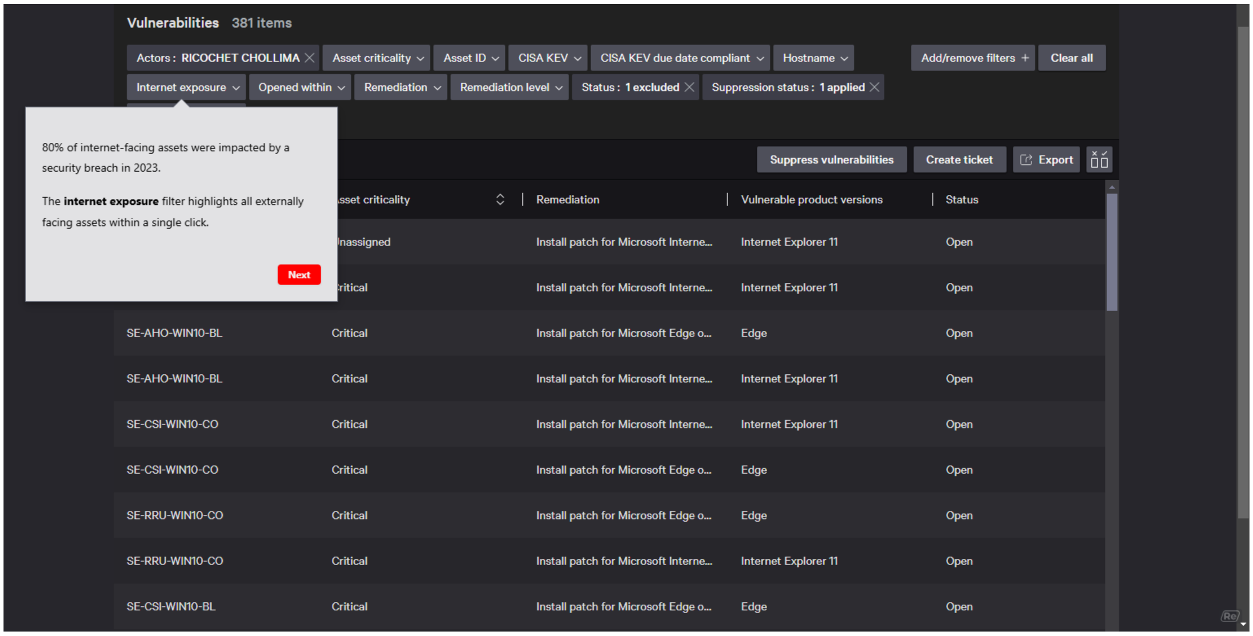
3:03 the next step in the investigation in
3:06 this case the process is immediately
3:08 blocked in the file quarantined by the
3:10 platform Falcon adversary intelligence
3:13 automatically detonates quarantined
3:15 files in a secure environment to
3:18 understand the severity score and risk
3:20 as part of the detection reviewing the
3:22 sandbox report enables you to surface
3:25 hidden ioc's that can be leveraged to
3:27 prevent future attacks now you can
3:31 proactively identify and remediate any
3:33 potentially impacted
3:35 systems Falcon adversary intelligence

English (auto-generated)

[48]

[48] https://www.youtube.com/watch?v=RrKQN8x2Ldc.

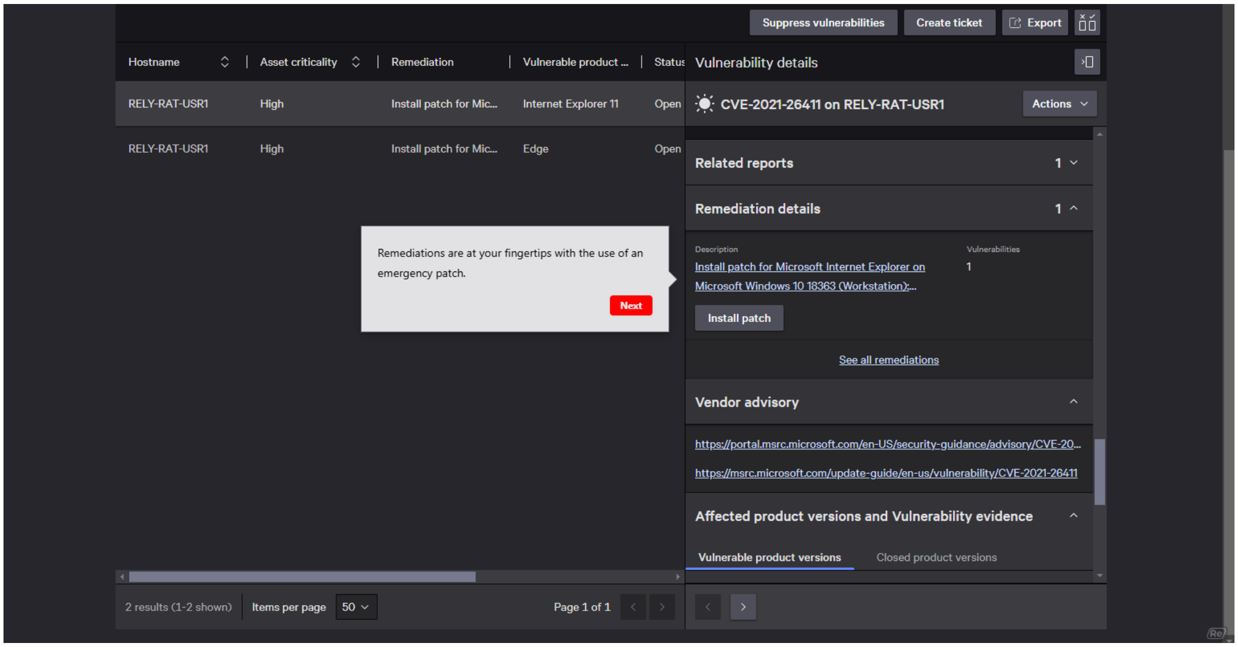
80. In another example for the Falcon Exposure Management module, 381 "Vulnerabilities" are detected for an exemplary computer environment. Included is the "Vulnerable product versions" (e.g., "Internet Explorer 11," "Edge") and "Remediation" (e.g., "Install patch") (altering a configuration of the computer system). "Remediations" include "emergency patch[es]" which "helps organizations deploy patches for high risk vulnerabilities." Related, data from "multiple CrowdStrike modules are compiled" to assess with vulnerabilities as well as detections and file integrity.



80% of internet-facing assets were impacted by a security breach in 2023.

The **internet exposure** filter highlights all externally facing assets within a single click.

	sset criticality	Remediation	Vulnerable product versions	Status
	nassigned	Install patch for Microsoft Interne...	Internet Explorer 11	Open
	ritical	Install patch for Microsoft Interne...	Internet Explorer 11	Open
SE-AHO-WIN10-BL	Critical	Install patch for Microsoft Edge o...	Edge	Open
SE-AHO-WIN10-BL	Critical	Install patch for Microsoft Interne...	Internet Explorer 11	Open
SE-CSI-WIN10-CO	Critical	Install patch for Microsoft Interne...	Internet Explorer 11	Open
SE-CSI-WIN10-CO	Critical	Install patch for Microsoft Edge o...	Edge	Open
SE-RRU-WIN10-CO	Critical	Install patch for Microsoft Edge o...	Edge	Open
SE-RRU-WIN10-CO	Critical	Install patch for Microsoft Interne...	Internet Explorer 11	Open
SE-CSI-WIN10-BL	Critical	Install patch for Microsoft Edge o...	Edge	Open



Hostname	Asset criticality	Remediation	Vulnerable product ...	Status
RELY-RAT-USR1	High	Install patch for Mic...	Internet Explorer 11	Open
RELY-RAT-USR1	High	Install patch for Mic...	Edge	Open

Remediations are at your fingertips with the use of an emergency patch.

CVE-2021-26411 on RELY-RAT-USR1

Related reports 1

Remediation details 1

Description: Install patch for Microsoft Internet Explorer on Microsoft Windows 10 18363 (Workstation):...

Vulnerabilities: 1

Vendor advisory

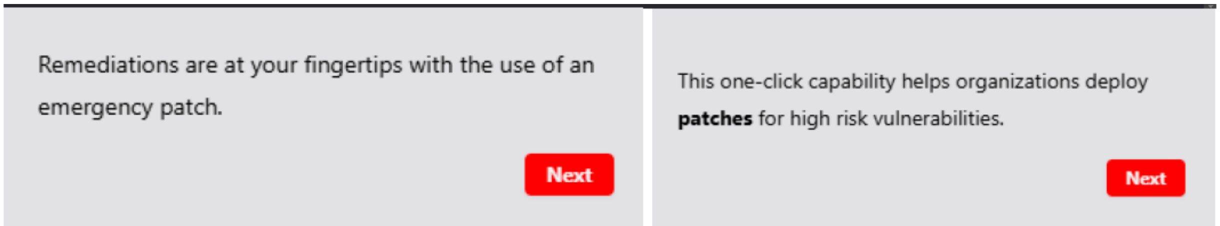
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-20...

https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2021-26411

Affected product versions and Vulnerability evidence

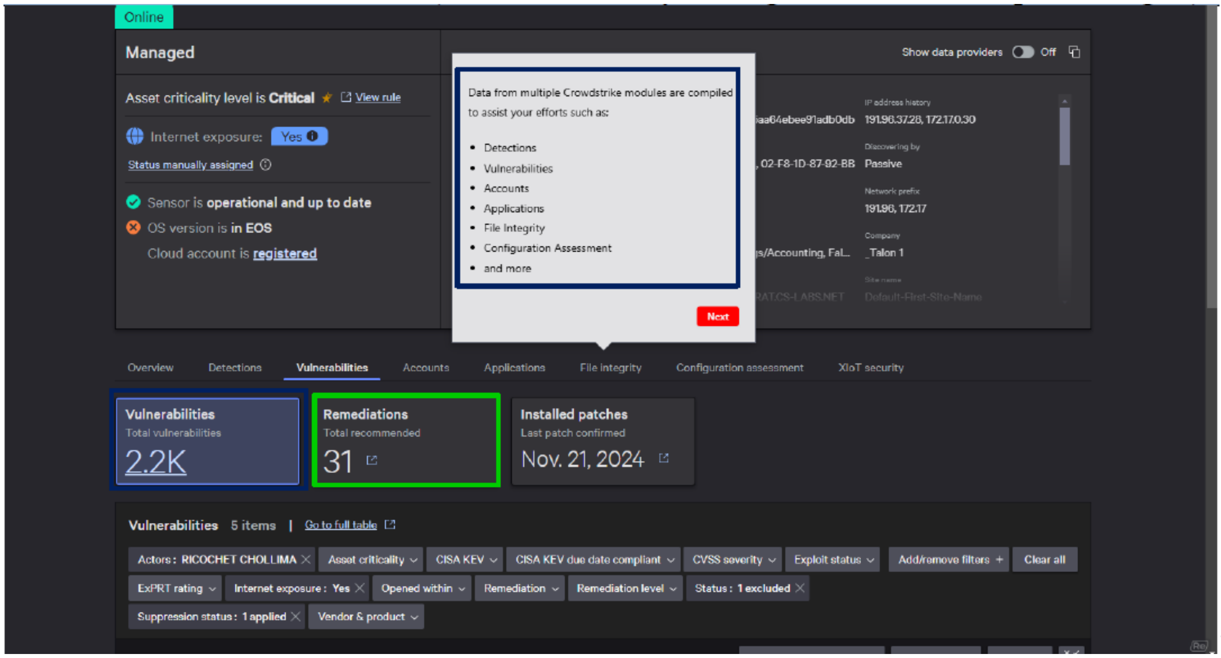
Vulnerable product versions Closed product versions

2 results (1-2 shown) Items per page 50 Page 1 of 1



Remediations are at your fingertips with the use of an emergency patch.

This one-click capability helps organizations deploy **patches** for high risk vulnerabilities.



Managed

Asset criticality level is **Critical** View rule

Internet exposure: Yes

Status manually assigned

Sensor is **operational and up to date**

OS version is **in EOS**

Cloud account is **registered**

Data from multiple Crowdstrike modules are compiled to assist your efforts such as:

- Detections
- Vulnerabilities
- Accounts
- Applications
- File Integrity
- Configuration Assessment
- and more

...aa64ebee91adb0db

IP address history: 191.96.37.28, 172.17.0.30

...02-F8-1D-87-92-BB

Discovering by: Passive

Network prefix: 191.96, 172.17

...s/Accounting, Fal...

Company: _Talon 1

...RAT.CS-LABS.NET

Site name: Default-First-Site-Name

Vulnerabilities — Total vulnerabilities: 2.2K

Remediations — Total recommended: 31

Installed patches — Last patch confirmed: Nov. 21, 2024

Vulnerabilities 5 items | Go to full table

Actors : RICOCHET CHOLLIMA ✕ | Asset criticality | CISA KEV | CISA KEV due date compliant | CVSS severity | Exploit status | Add/remove filters + | Clear all

ExPRT rating | Internet exposure : Yes ✕ | Opened within | Remediation | Remediation level | Status : 1 excluded ✕

Suppression status : 1 applied ✕ | Vendor & product

[49]

[49] https://www.crowdstrike.com/en-us/interactive-demos/falcon-exposure-management/.

81. Defendants have been aware of the ’385 Patent since at least the filing of this Complaint.

82. Defendants’ partners, customers, and end users of the Accused Products and corresponding systems and services directly infringe at least claim 8 of the ’385 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services.

83. Defendants have actively induced and are actively inducing infringement of at least claim 8 of the ’385 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that their acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendants encourage and induce customers to use CrowdStrike’s security software in a manner that infringes claim 8 of the ’385 Patent at least by offering and providing software that performs a method that infringes claim 8 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products.

84. Defendants encourage, instruct, direct, and/or require third parties—including their certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways.

85. Defendants further encourage and induce their customers to infringe at least claim 8 of the ’385 Patent: 1) by making their security services available on their website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to

marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including their CrowdStrike security software, and services in the United States.[50]

86. For example, on information and belief, Defendants share instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners.[51] On further information and belief, Defendants also provide customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner.[52]

87. Defendants and/or Defendants' partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendants and/or one of Defendants' partners, which obligates each customer to perform certain actions in order to use the Accused Products.[53] Further, in order to receive the benefit of Defendants' and/or their partners' continued technical support and their specialized knowledge and guidance of the operability of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '385 Patent.[54]

88. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each

[50] https://www.crowdstrike.com/en-us/; https://www.crowdstrike.com/en-us/partners/partner-program/.

[51] https://www.crowdstrike.com/en-us/free-trial-guide/; https://www.crowdstrike.com/en-us/free-trial-guide/start-and-install/.

[52] https://www.crowdstrike.com/contact-us/.

[53] https://www.crowdstrike.com/free-trial-guide/purchase/; https://www.crowdstrike.com/free-trial-guide/installation/).

[54] *See* https://www.crowdstrike.com/contact-us/.

customer through ongoing technical support, on information and belief, Defendants and/or Defendants' partners affirmatively aid and abet each customer's use of the Accused Products in a manner that performs the claimed method of, and infringes, the '385 Patent.

89. Plaintiff has suffered and continues to suffer damages as a result of Defendants' infringement of the '385 Patent. Defendants are therefore liable to Plaintiff under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiff for Defendants' infringement, but no less than a reasonable royalty.

90. Plaintiff, its predecessors-in-interest, and/or any licensees have satisfied all statutory obligations required to collect pre-filing damages for the full period allowed by law for infringement of the '385 Patent.

91. On information and belief, despite Defendants' knowledge of the Asserted Patents and Plaintiff's patented technology, Defendants made the deliberate decision to sell products and services that they knew infringe the Asserted Patents. Defendants' continued infringement of the '385 Patent with knowledge of the '385 Patent constitutes willful infringement.

SECOND CAUSE OF ACTION
(INFRINGEMENT OF THE '900 PATENT)

92. Plaintiff incorporates and realleges all of the above paragraphs as though fully set forth herein.

93. Defendants are not licensed (expressly or impliedly) or otherwise authorized to make, use, offer for sale, or sell any products or services that embody the inventions of the '900 Patent.

94. Defendants have infringed and continue to infringe, either literally and/or under the doctrine of equivalents, one or more claims of the '900 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this

Court. The Accused Products, including features of the Falcon Platform, at least when used for their ordinary and customary purposes, practice each element of at least claim 12 of the ’900 Patent.

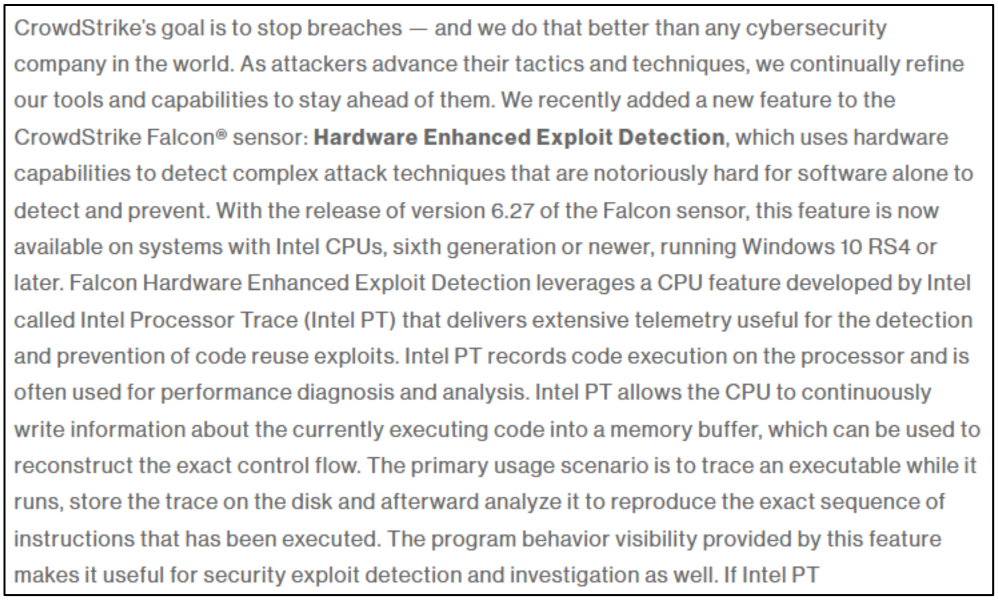
95. Claim 12 of the ’900 Patent recites:

> A method, comprising:
>
> configuring a processor for executing operations including:
>
> accessing data associated with a deep web forum, the data defining a topic for classification;
>
> extracting a set of features from the data as inputs for a machine classifier; and
>
> apply a machine classifier to the set of features to generate a prediction list of tags for classifying the topic, wherein the prediction list includes a prediction probability value for each tag of the plurality of tags; and
>
> adding all parent tags associated with a tag of the plurality of tags to the prediction list based on a comparison between the prediction probability value for the tag and a first predetermined threshold value.

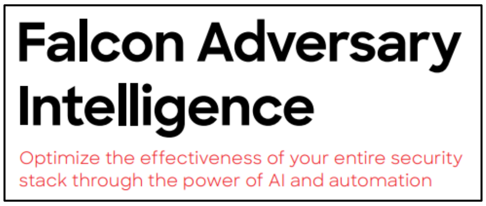
96. As illustrated in the example below,[55] the Falcon Platform embodies a system that includes each element of claim 12 of the ’900 Patent. For instance, the Falcon Platform performs a method including *configuring a processor for executing operations*. For example, the Falcon Platform’s lightweight Falcon sensor “consum[es] 1% or less of CPU [central processing unit]” power (a processor).[56] As a further example, the Falcon Platform includes “Hardware Enhanced Exploit Detection” features which uses processors to perform continuous monitoring and detection of complex attack techniques.

[55] The following examples are illustrative only and not intended to limit Plaintiff’s right to supplement or modify its allegations regarding the exemplary products or to allege that other CrowdStrike products infringe the ’900 Patent.

[56] https://www.crowdstrike.com/products/faq/

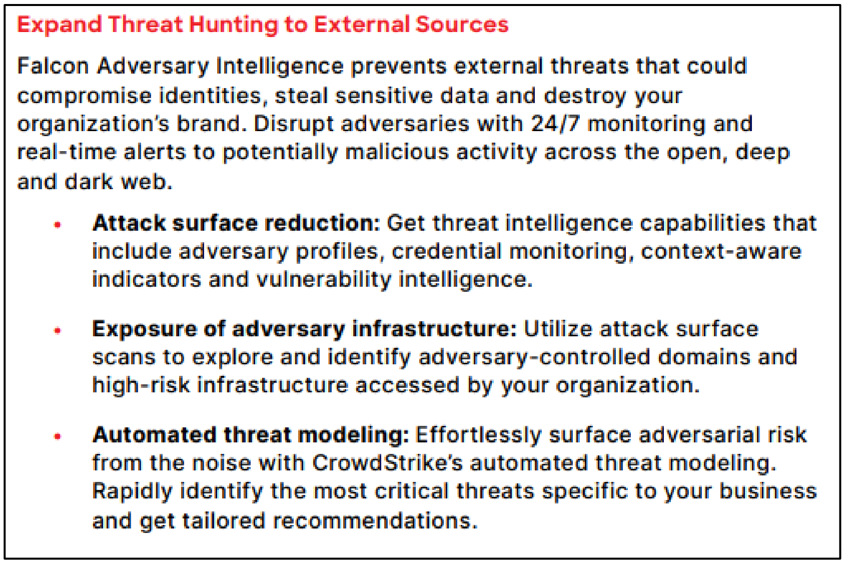

CrowdStrike's goal is to stop breaches — and we do that better than any cybersecurity company in the world. As attackers advance their tactics and techniques, we continually refine our tools and capabilities to stay ahead of them. We recently added a new feature to the CrowdStrike Falcon® sensor: **Hardware Enhanced Exploit Detection**, which uses hardware capabilities to detect complex attack techniques that are notoriously hard for software alone to detect and prevent. With the release of version 6.27 of the Falcon sensor, this feature is now available on systems with Intel CPUs, sixth generation or newer, running Windows 10 RS4 or later. Falcon Hardware Enhanced Exploit Detection leverages a CPU feature developed by Intel called Intel Processor Trace (Intel PT) that delivers extensive telemetry useful for the detection and prevention of code reuse exploits. Intel PT records code execution on the processor and is often used for performance diagnosis and analysis. Intel PT allows the CPU to continuously write information about the currently executing code into a memory buffer, which can be used to reconstruct the exact control flow. The primary usage scenario is to trace an executable while it runs, store the trace on the disk and afterward analyze it to reproduce the exact sequence of instructions that has been executed. The program behavior visibility provided by this feature makes it useful for security exploit detection and investigation as well. If Intel PT [57]

97. The Falcon Platform performs a method including *accessing data associated with a deep web forum, the data defining a topic for classification*. For instance, Falcon Adversary Intelligence is a Falcon Platform module that implements extended threat intelligence and dark web monitoring to Falcon Platform customers. Falcon Adversary Intelligence "[d]isrupt[s] adversaries with 24/7 monitoring and real-time alerts to potentially malicious activity across the open, deep and dark web" (e.g., *accessing data associated with a deep web forum*).


Falcon Adversary Intelligence

Optimize the effectiveness of your entire security stack through the power of AI and automation

[57] https://www.crowdstrike.com/blog/introducing-falcon-hardware-enhanced-exploit-detection/



Expand Threat Hunting to External Sources

Falcon Adversary Intelligence prevents external threats that could compromise identities, steal sensitive data and destroy your organization's brand. Disrupt adversaries with 24/7 monitoring and real-time alerts to potentially malicious activity across the open, deep and dark web.

- **Attack surface reduction:** Get threat intelligence capabilities that include adversary profiles, credential monitoring, context-aware indicators and vulnerability intelligence.
- **Exposure of adversary infrastructure:** Utilize attack surface scans to explore and identify adversary-controlled domains and high-risk infrastructure accessed by your organization.
- **Automated threat modeling:** Effortlessly surface adversarial risk from the noise with CrowdStrike's automated threat modeling. Rapidly identify the most critical threats specific to your business and get tailored recommendations.

[58]

98. The Falcon Platform includes further products and services for *accessing data associated with a deep web forum*, such as Falcon Adversary Intelligence Premium,[59] Falcon Adversary Overwatch,[60] and Falcon Intelligence Recon. Falcon Intelligence Recon "automatically collects data and monitors data from millions of restricted web pages, criminal forums and encrypted messaging platforms."[61] CrowdStrike further advertises its monitoring of several thousand deep-web sites.

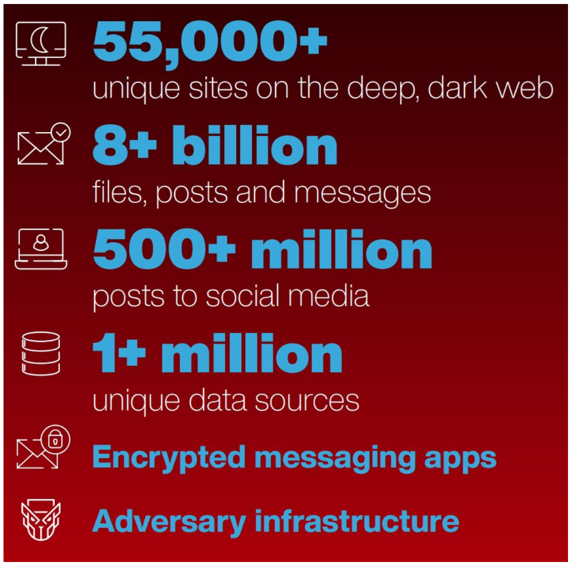
Falcon Intelligence Recon monitors the following:

[58] https://www.crowdstrike.com/wp-content/uploads/2024/04/Data-Sheet-_-Falcon-Adversary-Intelligence.pdf

[59] https://www.crowdstrike.com/wp-content/uploads/2024/02/falcon-adversary-intelligence-premium-data-sheet.pdf).

[60] https://www.crowdstrike.com/platform/threat-intelligence/adversary-overwatch/.

[61] https://www.crowdstrike.fr/wp-content/uploads/2021/08/crowdstrike-falcon-intelligence-recon.pdf.



55,000+
unique sites on the deep, dark web

8+ billion
files, posts and messages

500+ million
posts to social media

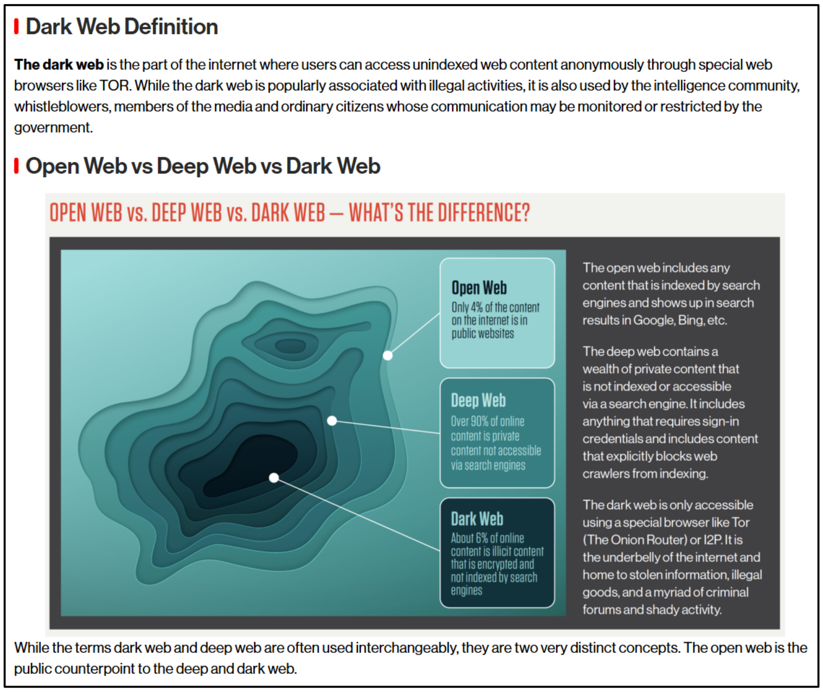
1+ million
unique data sources

Encrypted messaging apps

Adversary infrastructure

[62]

99. As described by CrowdStrike, the deep web comprises its subset, the dark web. CrowdStrike's monitoring of dark-web information forms a part of its analysis of the deep web.



Dark Web Definition

The dark web is the part of the internet where users can access unindexed web content anonymously through special web browsers like TOR. While the dark web is popularly associated with illegal activities, it is also used by the intelligence community, whistleblowers, members of the media and ordinary citizens whose communication may be monitored or restricted by the government.

Open Web vs Deep Web vs Dark Web

OPEN WEB vs. DEEP WEB vs. DARK WEB — WHAT'S THE DIFFERENCE?

Open Web
Only 4% of the content on the internet is in public websites

Deep Web
Over 90% of online content is private content not accessible via search engines

Dark Web
About 6% of online content is illicit content that is encrypted and not indexed by search engines

The open web includes any content that is indexed by search engines and shows up in search results in Google, Bing, etc.

The deep web contains a wealth of private content that is not indexed or accessible via a search engine. It includes anything that requires sign-in credentials and includes content that explicitly blocks web crawlers from indexing.

The dark web is only accessible using a special browser like Tor (The Onion Router) or I2P. It is the underbelly of the internet and home to stolen information, illegal goods, and a myriad of criminal forums and shady activity.

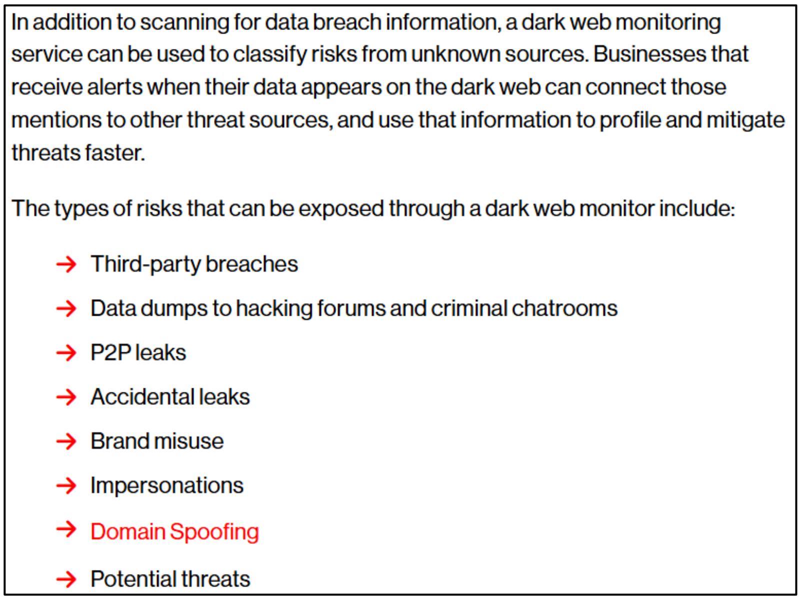
While the terms dark web and deep web are often used interchangeably, they are two very distinct concepts. The open web is the public counterpoint to the deep and dark web.

[63]

[62] https://www.crowdstrike.com/wp-content/uploads/2022/10/falcon-threat-intelligence-recon-infographic.pdf

[63] https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/dark-web/

100. The Falcon Platform's deep-web monitoring services (including Falcon Adversary Intelligence and Falcon Intelligence Recon mentioned above) categorize the content they collect. Various tags can be assigned based on the content category and form tag hierarchies (e.g., *the data defining a topic for classification*).



In addition to scanning for data breach information, a dark web monitoring service can be used to classify risks from unknown sources. Businesses that receive alerts when their data appears on the dark web can connect those mentions to other threat sources, and use that information to profile and mitigate threats faster.

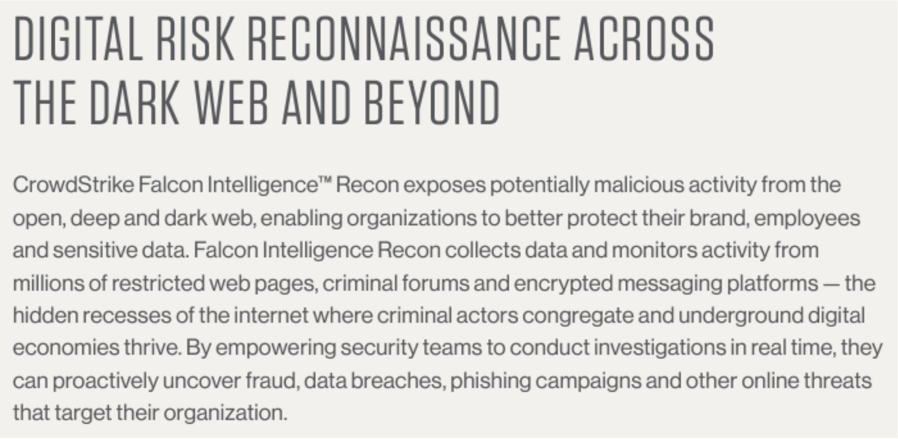
The types of risks that can be exposed through a dark web monitor include:

→ Third-party breaches
→ Data dumps to hacking forums and criminal chatrooms
→ P2P leaks
→ Accidental leaks
→ Brand misuse
→ Impersonations
→ Domain Spoofing
→ Potential threats

[64]

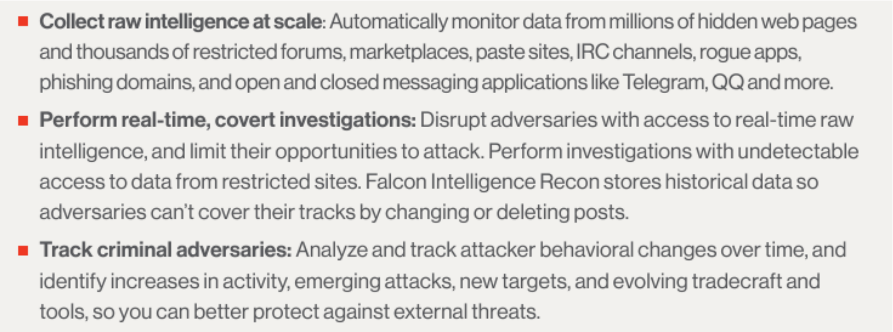
101. This data collection and monitoring reaches "the hidden recesses of the internet where criminal actors congregate." CrowdStrike customers can "[p]erform investigations with undetectable access to data from restricted sites." Falcon Intelligence Recon even "stores historical data so adversaries can't cover their tracks."

[64] https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/dark-web-monitoring/



DIGITAL RISK RECONNAISSANCE ACROSS THE DARK WEB AND BEYOND

CrowdStrike Falcon Intelligence™ Recon exposes potentially malicious activity from the open, deep and dark web, enabling organizations to better protect their brand, employees and sensitive data. Falcon Intelligence Recon collects data and monitors activity from millions of restricted web pages, criminal forums and encrypted messaging platforms — the hidden recesses of the internet where criminal actors congregate and underground digital economies thrive. By empowering security teams to conduct investigations in real time, they can proactively uncover fraud, data breaches, phishing campaigns and other online threats that target their organization.



- **Collect raw intelligence at scale**: Automatically monitor data from millions of hidden web pages and thousands of restricted forums, marketplaces, paste sites, IRC channels, rogue apps, phishing domains, and open and closed messaging applications like Telegram, QQ and more.
- **Perform real-time, covert investigations:** Disrupt adversaries with access to real-time raw intelligence, and limit their opportunities to attack. Perform investigations with undetectable access to data from restricted sites. Falcon Intelligence Recon stores historical data so adversaries can't cover their tracks by changing or deleting posts.
- **Track criminal adversaries:** Analyze and track attacker behavioral changes over time, and identify increases in activity, emerging attacks, new targets, and evolving tradecraft and tools, so you can better protect against external threats.

[65]

102. The Falcon Platform performs a method including *extracting a set of features from the data as inputs for a machine classifier*. For example, Falcon Adversary Intelligence implements "advanced threat intelligence" that includes information collected from "dark web monitoring" (*the data*) and extracts "context aware indicators" (*set of features*) for a "smarter, faster defense." As an example, Falcon Adversary Intelligence "is specifically designed to keep an eye on the dark web, providing critical insights into the activities of cybercriminals" found on "dark web forums" (*the data*). Indeed, Falcon Adversary Intelligence "provides real-time dark web monitoring for cybercrime activities, tracking malicious activity within criminal forums, criminal marketplaces, and underground communities" and uses "automated intelligence orchestration, contextual enrichment, and AI-native investigative tools" (*extract a set of features from the data*) to optimize

[65] https://www.crowdstrike.fr/wp-content/uploads/2021/08/crowdstrike-falcon-intelligence-recon.pdf

entire security stacks. (*See* https://www.crowdstrike.com/platform/threat-intelligence/adversary-intelligence/).

103. Furthermore, the Falcon Platform implements "feature vectors and metadata" for CrowdStrike's "machine learning model." "Feature vectors and metadata" from deep-web monitoring are sent to the "CrowdStrike Security Cloud" which is then fed into "CrowdStrike machine learning" (e.g., *as inputs for a machine classifier*).

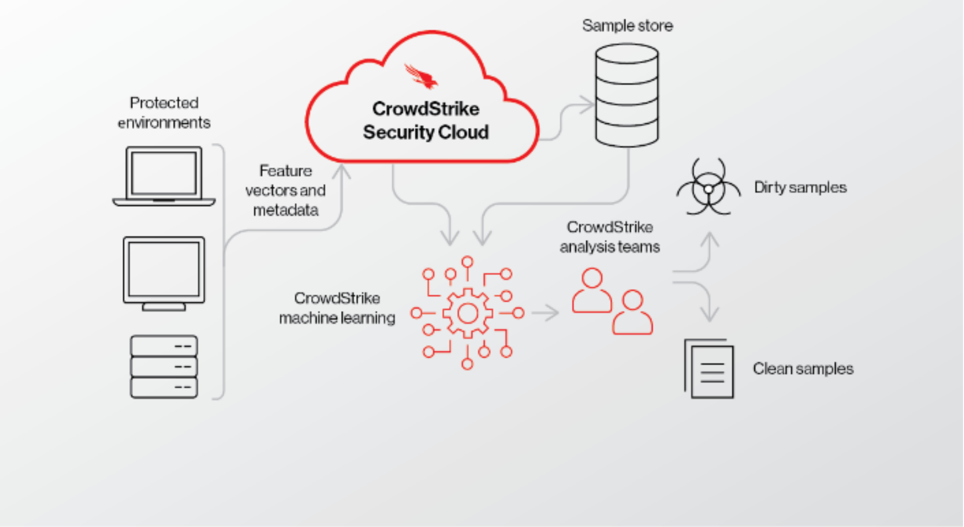
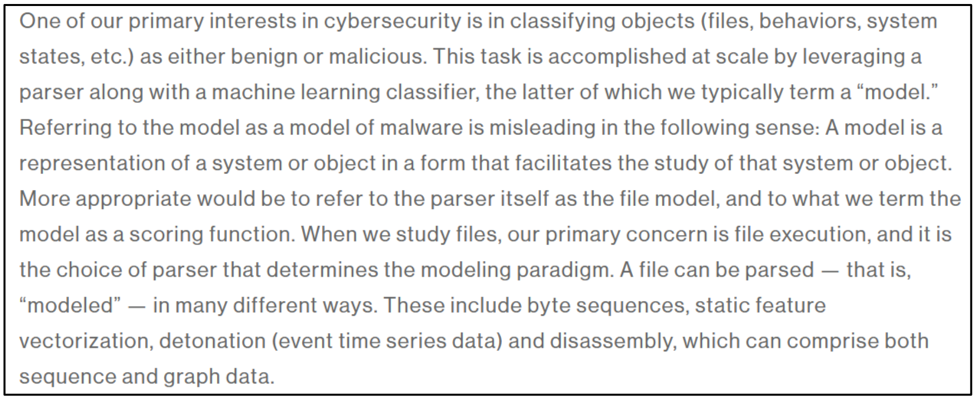

Sample store
Protected environments
CrowdStrike Security Cloud
Feature vectors and metadata
Dirty samples
CrowdStrike analysis teams
CrowdStrike machine learning
Clean samples

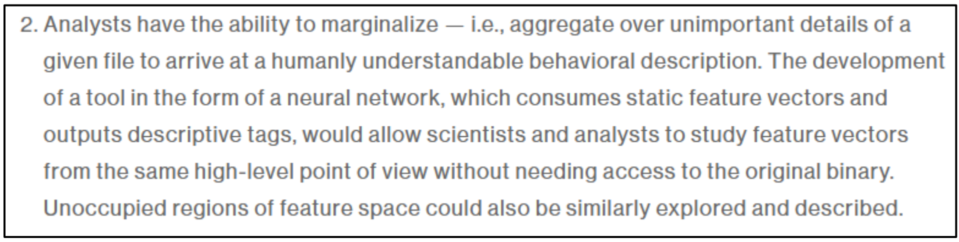
Figure 1. This flow describes how feature vectors and metadata are sent to the CrowdStrike Security Cloud and used against our machine learning model to help build better predictions. [66]

104. The Falcon Platform performs a method step that *appl*[ies] *a machine classifier to the set of features to generate a prediction list of tags for classifying the topic, wherein the prediction list includes a prediction probability value for each tag of the plurality of tags*. For instance, the Falcon Platform uses machine-learning models to classify data (*apply a machine classifier to the set of features to generate a prediction list of tags for classifying the topic*). Furthermore, the Falcon Platform uses a neural network to "consume[] static feature vectors and output[] descriptive tags" (*to generate a prediction list of tags for classifying the discussion*).

[66] https://www.crowdstrike.com/en-us/blog/how-crowdstrike-machine-learning-model-maximizes-detection-efficacy-using-the-cloud/



One of our primary interests in cybersecurity is in classifying objects (files, behaviors, system states, etc.) as either benign or malicious. This task is accomplished at scale by leveraging a parser along with a machine learning classifier, the latter of which we typically term a "model." Referring to the model as a model of malware is misleading in the following sense: A model is a representation of a system or object in a form that facilitates the study of that system or object. More appropriate would be to refer to the parser itself as the file model, and to what we term the model as a scoring function. When we study files, our primary concern is file execution, and it is the choice of parser that determines the modeling paradigm. A file can be parsed — that is, "modeled" — in many different ways. These include byte sequences, static feature vectorization, detonation (event time series data) and disassembly, which can comprise both sequence and graph data.

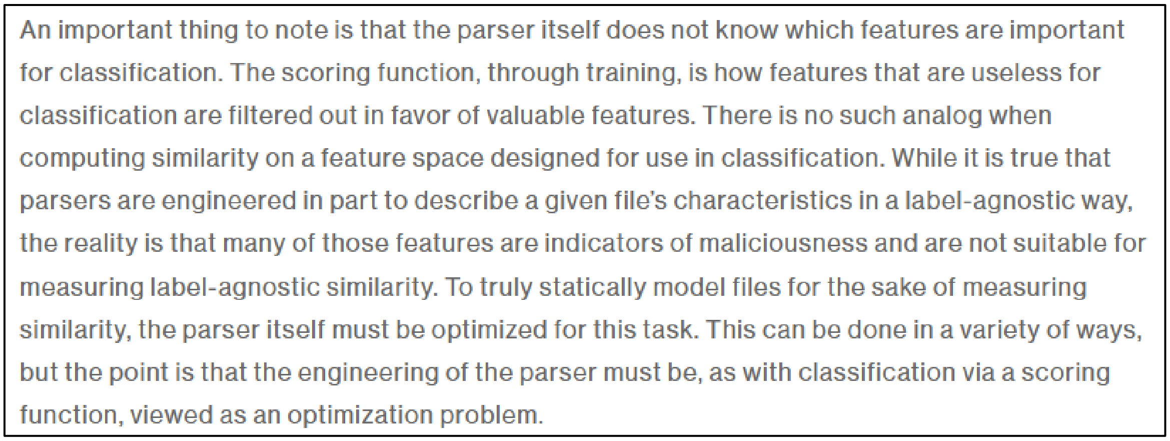


2. Analysts have the ability to marginalize — i.e., aggregate over unimportant details of a given file to arrive at a humanly understandable behavioral description. The development of a tool in the form of a neural network, which consumes static feature vectors and outputs descriptive tags, would allow scientists and analysts to study feature vectors from the same high-level point of view without needing access to the original binary. Unoccupied regions of feature space could also be similarly explored and described.

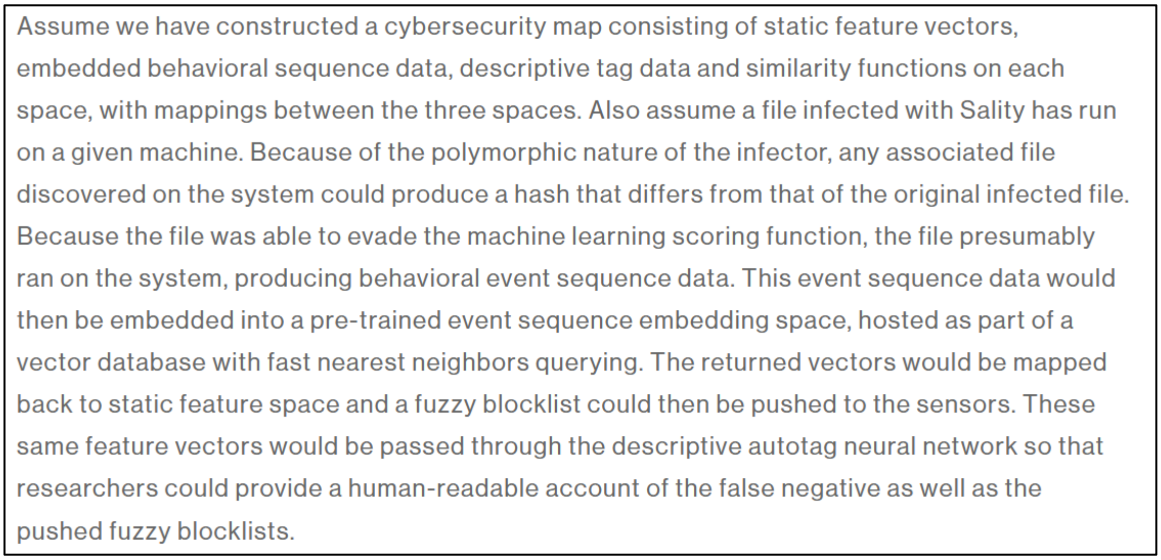
[67]

105. The Falcon Platform performs a method step of *adding all parent tags associated with a tag of the plurality of tags to the prediction list based on a comparison between the prediction probability value for the tag and a first predetermined threshold value*. The CrowdStrike Falcon Platform performs a scoring of tags its machine-learning tools assign to data features. This scoring feature helps classify the risks and assign tags based on the prediction probability value, or "how features that are useless for classification are filtered out in favor or valuable features." This includes a group of tags including parent tags. For example, "returned vectors" for an "associate file" are "mapped back to statice feature space and fuzzy blocklist." "These same feature vectors [are] passed through the descriptive autotag neural network" (*add all parent tags associated with a tag of the plurality of tags to the prediction list based on a comparison between the prediction probability value for the tag and a first predetermined threshold value*).

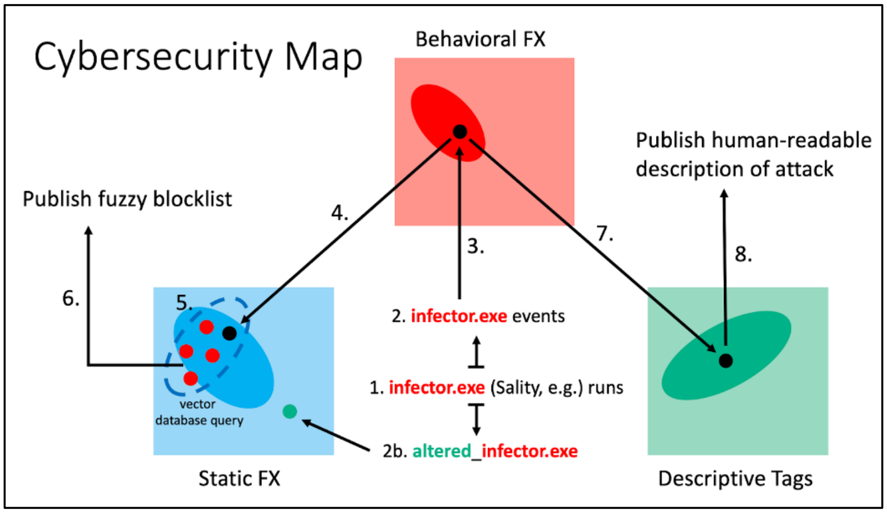
[67] https://www.crowdstrike.com/en-us/blog/using-similarity-based-mapping-to-prevent-breaches/



An important thing to note is that the parser itself does not know which features are important for classification. The scoring function, through training, is how features that are useless for classification are filtered out in favor of valuable features. There is no such analog when computing similarity on a feature space designed for use in classification. While it is true that parsers are engineered in part to describe a given file's characteristics in a label-agnostic way, the reality is that many of those features are indicators of maliciousness and are not suitable for measuring label-agnostic similarity. To truly statically model files for the sake of measuring similarity, the parser itself must be optimized for this task. This can be done in a variety of ways, but the point is that the engineering of the parser must be, as with classification via a scoring function, viewed as an optimization problem.



Assume we have constructed a cybersecurity map consisting of static feature vectors, embedded behavioral sequence data, descriptive tag data and similarity functions on each space, with mappings between the three spaces. Also assume a file infected with Sality has run on a given machine. Because of the polymorphic nature of the infector, any associated file discovered on the system could produce a hash that differs from that of the original infected file. Because the file was able to evade the machine learning scoring function, the file presumably ran on the system, producing behavioral event sequence data. This event sequence data would then be embedded into a pre-trained event sequence embedding space, hosted as part of a vector database with fast nearest neighbors querying. The returned vectors would be mapped back to static feature space and a fuzzy blocklist could then be pushed to the sensors. These same feature vectors would be passed through the descriptive autotag neural network so that researchers could provide a human-readable account of the false negative as well as the pushed fuzzy blocklists.



[68]

[68] https://www.crowdstrike.com/en-us/blog/using-similarity-based-mapping-to-prevent-breaches/

106. Defendants have been aware of the ’900 Patent since at least the filing of this Complaint.

107. Defendants’ partners, customers, and end users of the Accused Products and corresponding systems and services directly and indirectly infringe at least claim 12 of the ’900 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services.

108. Defendants have actively induced and are actively inducing infringement of at least claim 12 of the ’900 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that their acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendants encourage and induce customers to use CrowdStrike’s security software in a manner that infringes claim 12 of the ’900 Patent at least by offering and providing software that performs a method that infringes claim 12 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products.

109. Defendants encourage, instruct, direct, and/or require third parties—including their certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways.

110. Defendants further encourage and induce their customers to infringe at least claim 12 of the ’900 Patent: 1) by making their security services available on their website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to

marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including their CrowdStrike security software, and services in the United States.[69]

111. For example, on information and belief, Defendants share instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners.[70] On further information and belief, Defendants also provide customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner.[71]

112. Defendants and/or Defendants' partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendants and/or one of Defendants' partners, which obligates each customer to perform certain actions in order to use the Accused Products.[72] Further, in order to receive the benefit of Defendants' and/or their partners' continued technical support and their specialized knowledge and guidance of the operability of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '900 Patent.[73]

113. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each

[69] https://www.crowdstrike.com/en-us/; https://www.crowdstrike.com/en-us/partners/partner-program/.
[70] https://www.crowdstrike.com/en-us/free-trial-guide/; https://www.crowdstrike.com/en-us/free-trial-guide/start-and-install/.
[71] https://www.crowdstrike.com/contact-us/.
[72] https://www.crowdstrike.com/free-trial-guide/purchase/; https://www.crowdstrike.com/free-trial-guide/installation/).
[73] *See* https://www.crowdstrike.com/contact-us/.

customer through ongoing technical support, on information and belief, Defendants and/or Defendants' partners affirmatively aid and abet each customer's use of the Accused Products in a manner that performs the claimed method of, and infringes, the '900 Patent.

114. Plaintiff has suffered and continues to suffer damages as a result of Defendants' infringement of the '900 Patent. Defendants are therefore liable to Plaintiff under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiff for Defendants' infringement, but no less than a reasonable royalty.

115. Plaintiff, its predecessors-in-interest, and/or any licensees have satisfied all statutory obligations required to collect pre-filing damages for the full period allowed by law for infringement of the '900 Patent.

116. On information and belief, despite Defendants' knowledge of the Asserted Patents and Plaintiff's patented technology, Defendants made the deliberate decision to sell products and services that they knew infringe the Asserted Patents. Defendants' continued infringement of the '900 Patent with knowledge of the '900 Patent constitutes willful infringement.

THIRD CAUSE OF ACTION
(INFRINGEMENT OF THE '831 PATENT)

117. Plaintiff incorporates and realleges all of the above paragraphs as though fully set forth herein.

118. Defendants are not licensed (expressly or impliedly) or otherwise authorized to make, use, offer for sale, or sell any products or services that embody the inventions of the '831 Patent.

119. Defendants have infringed and continue to infringe, either literally and/or under the doctrine of equivalents, one or more claims of the '831 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this

Court. The Accused Products, including features of the Falcon Platform, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the ’831 Patent.

120. Claim 1 of the ’831 Patent recites:

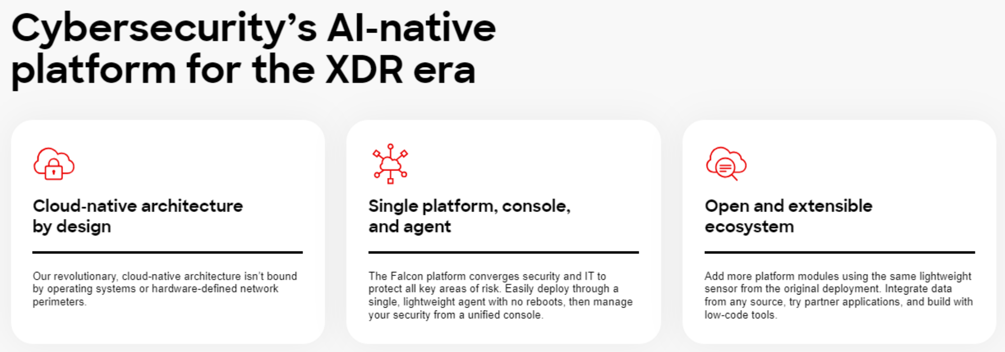
> One or more non-transitory computer-readable storage media storing instructions which, when executed by at least one processor, cause the at least one processor to perform operations comprising:
>
> in one or more layers of a convolutional neural network (CNN), performing a first iteration that includes computing a value based on a first set of most significant bits (MSBs) for each of a plurality of data sets;
>
> examining a first set of values computed for the plurality of data sets in the first iteration to determine whether a maximum value is present among the first set of values;
>
> responsive to identifying the maximum value, performing a full precision computation of the value for a data set, of the plurality of data sets, that exhibited the maximum value; and
>
> propagating the full precision computation of the value to a subsequent layer of the CNN.

121. As illustrated in the example below,[74] Falcon Platform embodies each element of claim 1 of the ’831 Patent. To the extent that the preamble is limiting, the Falcon Platform embodies the claimed *one or more non-transitory computer-readable storage media storing instructions which, when executed by at least one processor, cause the at least one processor to perform operations*. For instance, the Falcon Platform is a cloud-based SaaS for next-generation antivirus (“NGAV”) and endpoint detection and response (“EDR”). The Falcon Platform is made up of numerous modules that provide antivirus and related SaaS services. For example, Falcon Prevent is the core antivirus or NGAV module of the Falcon Platform and is included in every Falcon Platform subscription and bundle as shown by the red check marks for Falcon Go, Falcon

[74] The following examples are illustrative only and not intended to limit Plaintiff’s right to supplement or modify its allegations regarding the exemplary products or to allege that other CrowdStrike products infringe the ’831 Patent.

Pro, Falcon Enterprise, and Falcon Complete. Falcon Prevent "[p]rotects against all types of threat, from malware and ransomware to sophisticated attacks." (See https://www.crowdstrike.com/products/faq/).

122. The Falcon Platform is implemented on endpoint computers using a software called the Falcon Sensor or Falcon Agent that both protects computers and supports the Falcon Platform's cloud infrastructure. Using a "[s]ingle platform, console, and agent," the Falcon Platform "manage[s] . . . security from a unified console" and is "[e]asily deploy[ed] through a single, lightweight agent with no reboots."



Cybersecurity's AI-native platform for the XDR era

Cloud-native architecture by design

Our revolutionary, cloud-native architecture isn't bound by operating systems or hardware-defined network perimeters.

Single platform, console, and agent

The Falcon platform converges security and IT to protect all key areas of risk. Easily deploy through a single, lightweight agent with no reboots, then manage your security from a unified console.

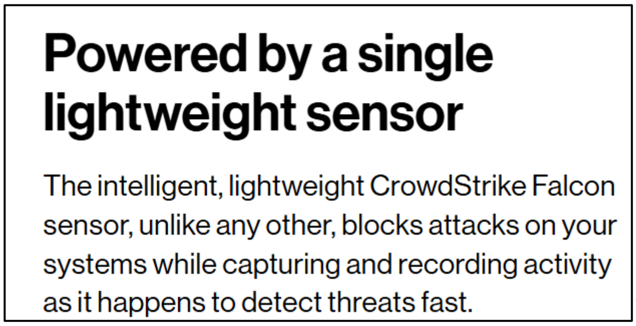
Open and extensible ecosystem

Add more platform modules using the same lightweight sensor from the original deployment. Integrate data from any source, try partner applications, and build with low-code tools.

123. The Falcon Sensor "is extremely lightweight (consuming 1% or less of CPU) (when executed by at least one processor, cause the at least one processor to perform operations) and unobtrusive and supports numerous computer operating systems including Windows, Mac, and Linux platforms. The Falcon Platform also support cloud computer environments and assets on cloud-based platforms such as Amazon Web Services.[75] The Falcon Platform "lightweight sensor" is installed on computer devices and stored on non-transitory computer-readable media, such as hard drives. It is the "foundation of [CrowdStrike's] next-generation endpoint protection" and "blocks attacks . . . while capturing and recording activity" (e.g., *one or more non-transitory*

[75] *See* https://www.crowdstrike.com/products/faq/.

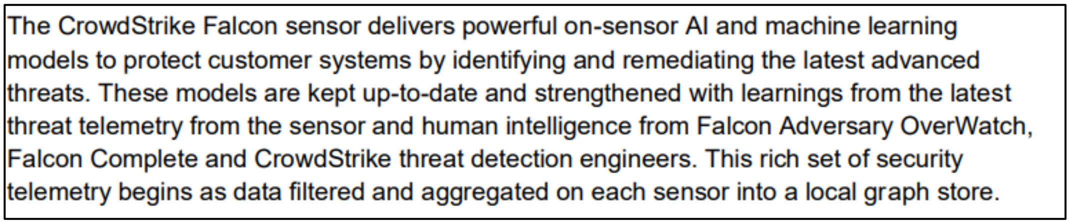
computer-readable storage media storing instructions). It also delivers "powerful on-sensor AI and machine learning models."



Powered by a single lightweight sensor

The intelligent, lightweight CrowdStrike Falcon sensor, unlike any other, blocks attacks on your systems while capturing and recording activity as it happens to detect threats fast.

[76]



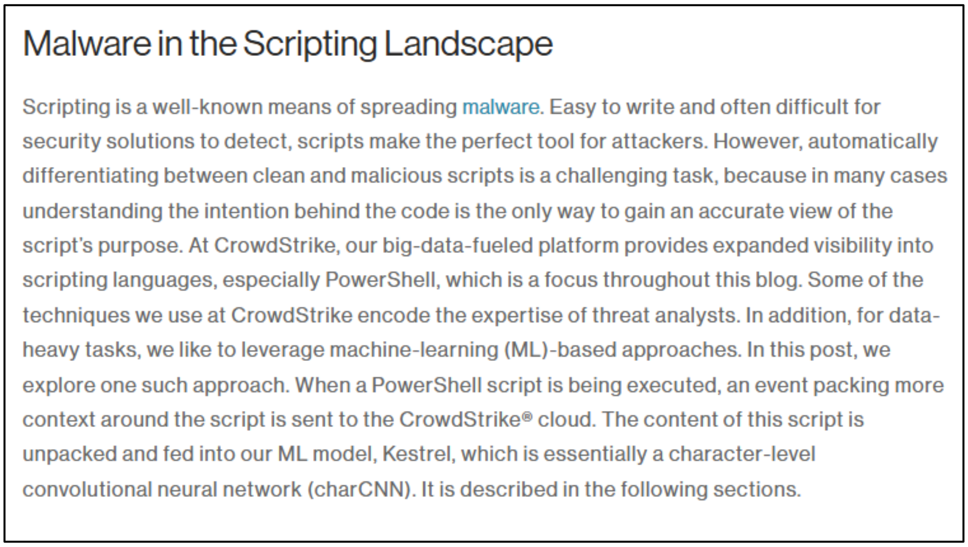
The CrowdStrike Falcon sensor delivers powerful on-sensor AI and machine learning models to protect customer systems by identifying and remediating the latest advanced threats. These models are kept up-to-date and strengthened with learnings from the latest threat telemetry from the sensor and human intelligence from Falcon Adversary OverWatch, Falcon Complete and CrowdStrike threat detection engineers. This rich set of security telemetry begins as data filtered and aggregated on each sensor into a local graph store.

[77]

124. The Falcon Platform embodies one or more non-transitory computer-readable storage media storing instructions which, when executed by at least one processor, cause the at least one processor to perform operations comprising "*in one or more layers of a convolutional neural network (CNN), performing a first iteration that includes computing a value based on a first set of most significant bits (MSBs) for each of a plurality of data sets*." For instance, the Falcon Platform implements a character-level convolutional neural network (charCNN) called Kestrel for detecting malware in scripts such as PowerShell. "When a PowerShell script is being executed . . . [t]he content of this script is unpacked and fed into [CrowdStrike's] ML model, Kestrel" (e.g., *for each of a plurality of data sets*). Because Kestrel is "lightweight . . . the model can be deployed anywhere" and it "has more interpretability due to its convolutional layers that keep some spatial clues on the patterns selected. This makes it possible to reverse the learning process and extract

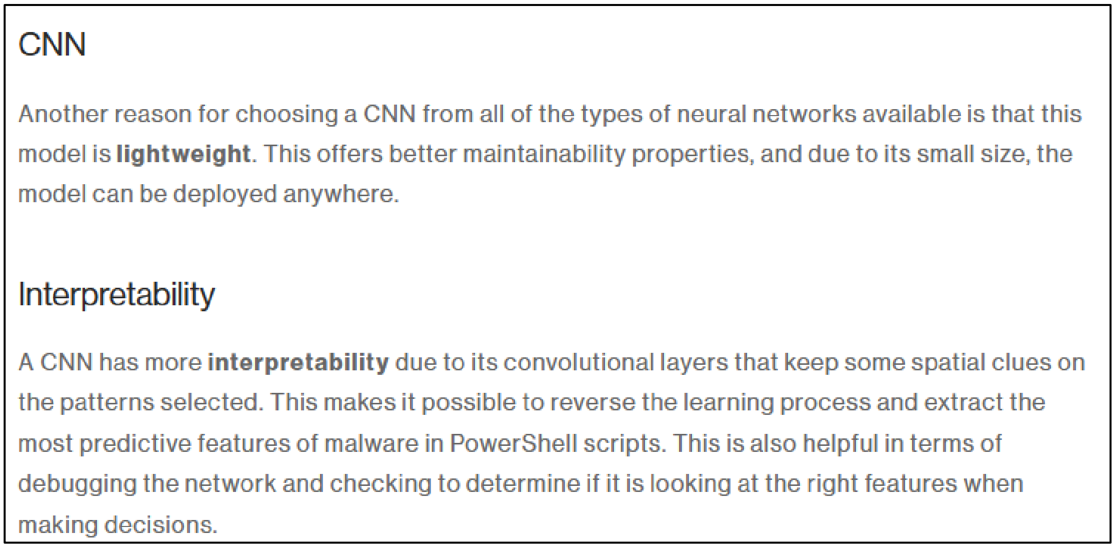
[76] *See* https://www.crowdstrike.com/products/trials/try-falcon-prevent/.
[77] https://www.crowdstrike.com/en-us/blog/using-similarity-based-mapping-to-prevent-breaches/

the most predictive features of malware in PowerShell scripts" (e.g., *performing a first iteration that includes computing a value based on a first set of most significant bits (MSBs)*).



Malware in the Scripting Landscape

Scripting is a well-known means of spreading malware. Easy to write and often difficult for security solutions to detect, scripts make the perfect tool for attackers. However, automatically differentiating between clean and malicious scripts is a challenging task, because in many cases understanding the intention behind the code is the only way to gain an accurate view of the script's purpose. At CrowdStrike, our big-data-fueled platform provides expanded visibility into scripting languages, especially PowerShell, which is a focus throughout this blog. Some of the techniques we use at CrowdStrike encode the expertise of threat analysts. In addition, for data-heavy tasks, we like to leverage machine-learning (ML)-based approaches. In this post, we explore one such approach. When a PowerShell script is being executed, an event packing more context around the script is sent to the CrowdStrike® cloud. The content of this script is unpacked and fed into our ML model, Kestrel, which is essentially a character-level convolutional neural network (charCNN). It is described in the following sections.



CNN

Another reason for choosing a CNN from all of the types of neural networks available is that this model is **lightweight**. This offers better maintainability properties, and due to its small size, the model can be deployed anywhere.

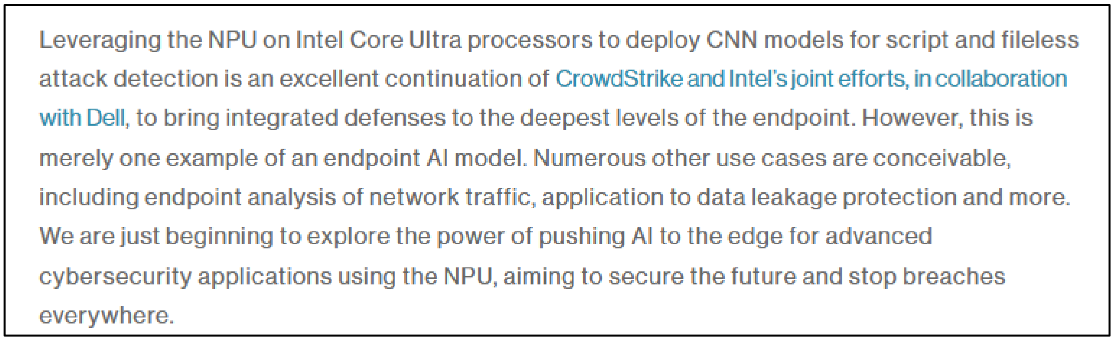
Interpretability

A CNN has more **interpretability** due to its convolutional layers that keep some spatial clues on the patterns selected. This makes it possible to reverse the learning process and extract the most predictive features of malware in PowerShell scripts. This is also helpful in terms of debugging the network and checking to determine if it is looking at the right features when making decisions.

[78]

125. Relatedly, CrowdStrike has begun a process to "to deploy CNN models for script and fileless attack detection" to "endpoints."

[78] https://www.crowdstrike.com/en-us/blog/malware-detection-with-charcnns-and-powershell-scripts/



Leveraging the NPU on Intel Core Ultra processors to deploy CNN models for script and fileless attack detection is an excellent continuation of CrowdStrike and Intel's joint efforts, in collaboration with Dell, to bring integrated defenses to the deepest levels of the endpoint. However, this is merely one example of an endpoint AI model. Numerous other use cases are conceivable, including endpoint analysis of network traffic, application to data leakage protection and more. We are just beginning to explore the power of pushing AI to the edge for advanced cybersecurity applications using the NPU, aiming to secure the future and stop breaches everywhere. [79]

126. In another example, CrowdStrike "use[s] the last convolutional layer to obtain high-level semantics that are class-specific (i.e., malware is of interest in our case) with the spatial localization in the given input" (e.g., *performing a first iteration that includes computing a value based on a first set of most significant bits (MSBs)*). This is important for "highlight[ing] the features (words/characters/n-grams) that are the most predictive of a class of interest which, in [CrowdStrike's] case, would be malware."[80] In another example, for using a convolutional neural network for classifying (identifying) malware families, the "main challenge . . . is the large size of modern binaries" because "convolution operations on long sequences of bytes are resource-intensive" (e.g., *for each of a plurality of data sets*). CrowdStrike "use[s] strides small enough that convolutional filters overlap the input data," (e.g., *in one or more layers of a convolutional neural network (CNN)*), and instead of "process[ing] all of the file at once", CrowdStrike software "only pull bytes from the entry point to the end of its section" to "dramatically reduce[] the resources consumed" because "the bytes following entry point are very relevant to the family, whereas other sections of a file could be less relevant because they comprise boilerplate functionality, compressed data or similarly unhelpful information" (e.g., *most significant bits (MSBs)*). These bytes are

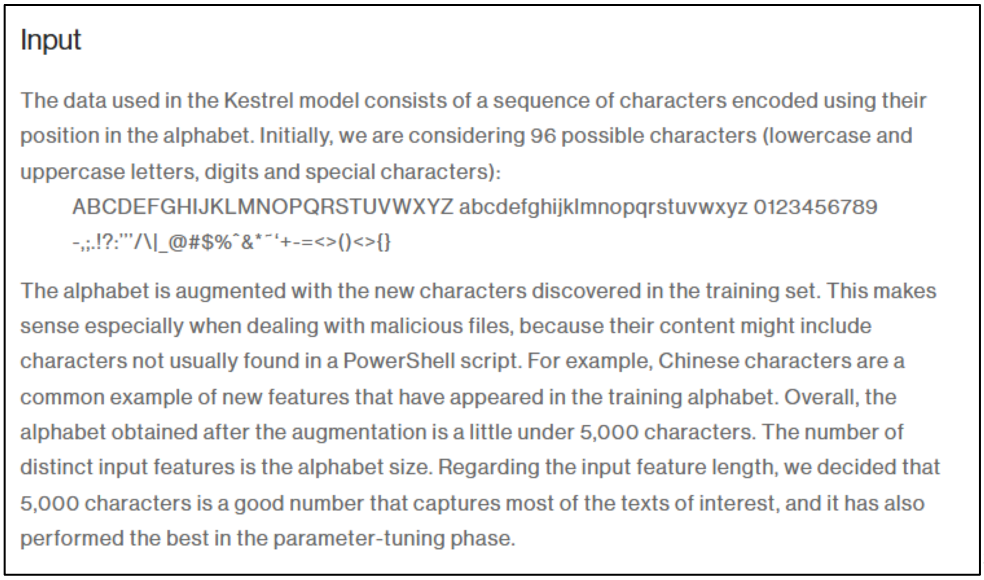
[79] https://www.crowdstrike.com/en-us/blog/crowdstrike-and-intel-research-advance-endpoint-security/

[80] https://www.crowdstrike.com/en-us/blog/malware-through-the-eyes-of-a-convolutional-neural-network.

analyzed to identify malware families using family embedding features (e.g., *performing a first iteration that includes computing a value*).[81]

127. The Falcon Platform embodies one or more non-transitory computer-readable storage media storing instructions which, when executed by at least one processor, cause the at least one processor to perform operations comprising "*examining a first set of values computed for the plurality of data sets in the first iteration to determine whether a maximum value is present among the first set of values*." For instance, the Kestrel charCNN used for scripts initially considers characters. Then the "alphabet is augmented with the new characters discovered in the training set. This makes sense especially when dealing with malicious files, because their content might include characters not usually found in a PowerShell script" (e.g., *examining a first set of values computed for the plurality of data sets in the first iteration*). Regarding the input feature length, CrowdStrike uses "5,000 characters [as] a good number that captures most of the texts of interest" (e.g., *to determine whether a maximum value is present*).

[81] *See* https://www.crowdstrike.com/en-us/blog/convolutional-neural-networks-are-male-models-for-pe-malware/.



Input

The data used in the Kestrel model consists of a sequence of characters encoded using their position in the alphabet. Initially, we are considering 96 possible characters (lowercase and uppercase letters, digits and special characters):

ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789
-,;.!?:'"/\|_@#$%ˆ&*˜'+-=<>()<>{}

The alphabet is augmented with the new characters discovered in the training set. This makes sense especially when dealing with malicious files, because their content might include characters not usually found in a PowerShell script. For example, Chinese characters are a common example of new features that have appeared in the training alphabet. Overall, the alphabet obtained after the augmentation is a little under 5,000 characters. The number of distinct input features is the alphabet size. Regarding the input feature length, we decided that 5,000 characters is a good number that captures most of the texts of interest, and it has also performed the best in the parameter-tuning phase.

[82]

128. In another example, CrowdStrike "use[s] the last convolutional layer to obtain high-level semantics that are class-specific . . . for "highlight[ing] the features (words/characters/n-grams) that are the most predictive of a class of interest which, in [CrowdStrike's] case, would be malware." Other verifications" are used to "reduc[e] the number of unclear explanations due to low model accuracy or text ambiguity . . . tak[ing] only samples that are correctly classified, with a confidence level above . . . 0.999" (e.g., *determine whether a maximum value is present among the first set of values*). (*See* https://www.crowdstrike.com/en-us/blog/malware-through-the-eyes-of-a-convolutional-neural-network/). In a further example, CrowdStrike uses convolutional neural networks for classifying (identifying) malware families. The Falcon Platform implements a "family embedding features" to make a "classification decision" wherein, the classification decision refers to the use of a decision threshold value to classify the samples. The process of comparing embedding features with a decision threshold to classify a dataset as benign or

[82] https://www.crowdstrike.com/en-us/blog/malware-detection-with-charcnns-and-powershell-scripts/

malicious in cybersecurity "examines a first set of values computed for the plurality of data sets in the first iteration to determine whether a maximum value is present."[83]

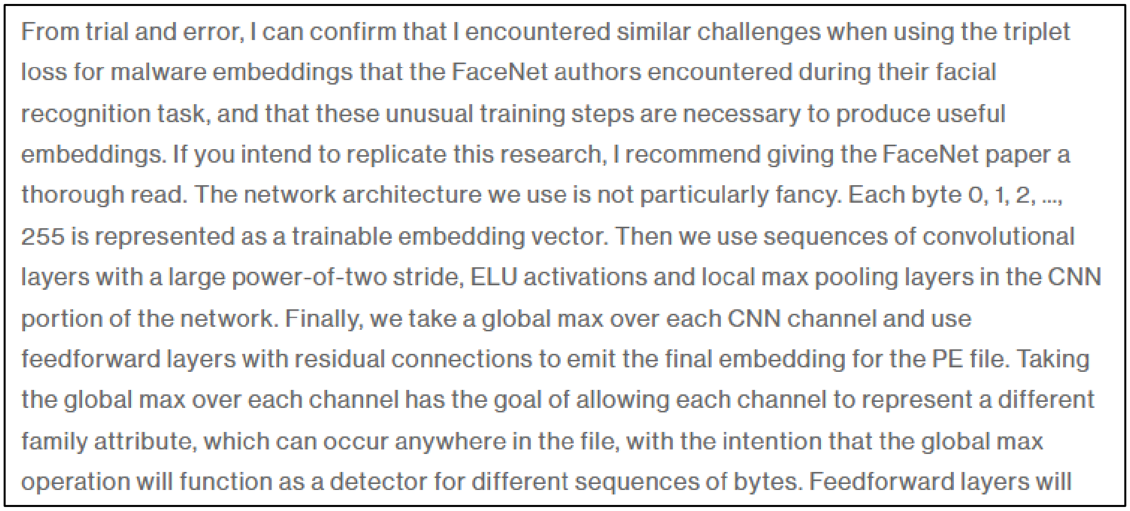
129. The Falcon Platform embodies one or more non-transitory computer-readable storage media storing instructions which, when executed by at least one processor, cause the at least one processor to perform operations comprising "*responsive to identifying the maximum value, performing a full precision computation of the value for a data set, of the plurality of data sets, that exhibited the maximum value*." For instance, the Falcon Platform's Kestrel (charCNN) model "use[s] an embedding layer with the aim of representing the indexes used for characters as continuous vectors that are more meaningful in terms of the categories they represent" (e.g., *responsive to identifying the maximum value*). The "computational flow starts with embedding the sequence of characters considered for each sample into a 5,000 x 128 floating point matrix" with each character being "mapped into a 128-dimensional embedding space" (e.g., *performing a full precision computation of the value for a data set, of the plurality of data sets, that exhibited the maximum value*).[84]

130. Finally, the Falcon Platform embodies one or more non-transitory computer-readable storage media storing instructions which, when executed by at least one processor, cause the at least one processor to perform operations comprising "*propagating the full precision computation of the value to a subsequent layer of the CNN*." For instance, the Falcon Platform's Kestrel (charCNN) model implements "temporal 1D max pooling allows [CrowdStrike Falcon] to train deeper models through the selection of only the relevant feature maps retrieved from the

[83] *See* https://www.crowdstrike.com/en-us/blog/convolutional-neural-networks-are-male-models-for-pe-malware/.

[84] *See* https://www.crowdstrike.com/en-us/blog/malware-detection-with-charcnns-and-powershell-scripts/.

convolutional modules" (e.g., *propagating the full precision computation of the value to a subsequent layer of the CNN*).[85] In another example, the CrowdStrike Falcon Platform use of feedforward layers after the global max pooling to generate the final embedding of the file which indicates that *the full precision computation of the value is propagated to a subsequent layer of the CNN*.



From trial and error, I can confirm that I encountered similar challenges when using the triplet loss for malware embeddings that the FaceNet authors encountered during their facial recognition task, and that these unusual training steps are necessary to produce useful embeddings. If you intend to replicate this research, I recommend giving the FaceNet paper a thorough read. The network architecture we use is not particularly fancy. Each byte 0, 1, 2, ..., 255 is represented as a trainable embedding vector. Then we use sequences of convolutional layers with a large power-of-two stride, ELU activations and local max pooling layers in the CNN portion of the network. Finally, we take a global max over each CNN channel and use feedforward layers with residual connections to emit the final embedding for the PE file. Taking the global max over each channel has the goal of allowing each channel to represent a different family attribute, which can occur anywhere in the file, with the intention that the global max operation will function as a detector for different sequences of bytes. Feedforward layers will

[86]

131. Defendants have been aware of the '831 Patent since at least the filing of this Complaint.

132. Defendants' partners, customers, and end users of the Accused Products and corresponding systems and services directly infringe at least claim 1 of the '831 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services.

133. Defendants have actively induced and are actively inducing infringement of at least claim 1 of the '831 Patent with specific intent to induce infringement, and/or willful blindness to

[85] *See* https://www.crowdstrike.com/en-us/blog/malware-detection-with-charcnns-and-powershell-scripts/.

[86] https://www.crowdstrike.com/en-us/blog/convolutional-neural-networks-are-male-models-for-pe-malware/

the possibility that their acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendants encourage and induce customers to use CrowdStrike's security software in a manner that infringes claim 1 of the '831 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products.

134. Defendants encourage, instruct, direct, and/or require third parties—including their certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways.

135. Defendants further encourage and induce their customers to infringe at least claim 1 of the '831 Patent: 1) by making their security services available on their website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including their CrowdStrike security software, and services in the United States.[87]

136. For example, on information and belief, Defendants share instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners.[88] On further information and belief, Defendants also provide customer service and technical support to purchasers of the Accused Products and

[87] https://www.crowdstrike.com/en-us/; https://www.crowdstrike.com/en-us/partners/partner-program/.
[88] https://www.crowdstrike.com/en-us/free-trial-guide/; https://www.crowdstrike.com/en-us/free-trial-guide/start-and-install/.

corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner.[89]

137. Defendants and/or Defendants' partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendants and/or one of Defendants' partners, which obligates each customer to perform certain actions in order to use the Accused Products.[90] Further, in order to receive the benefit of Defendants' and/or their partners' continued technical support and their specialized knowledge and guidance of the operability of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '831 Patent.[91]

138. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendants and/or Defendants' partners affirmatively aid and abet each customer's use of the Accused Products in a manner that performs the claimed method of, and infringes, the '831 Patent.

139. Plaintiff has suffered and continues to suffer damages as a result of Defendants' infringement of the '831 Patent. Defendants are therefore liable to Plaintiff under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiff for Defendants' infringement, but no less than a reasonable royalty.

[89] https://www.crowdstrike.com/contact-us/.

[90] https://www.crowdstrike.com/free-trial-guide/purchase/; https://www.crowdstrike.com/free-trial-guide/installation/).

[91] https://www.crowdstrike.com/contact-us/

140. Plaintiff, its predecessors-in-interest, and/or any licensees have satisfied all statutory obligations required to collect pre-filing damages for the full period allowed by law for infringement of the ’831 Patent.

141. On information and belief, despite Defendants’ knowledge of the Asserted Patents and Plaintiff’s patented technology, Defendants made the deliberate decision to sell products and services that they knew infringe the Asserted Patents. Defendants’ continued infringement of the ’831 Patent with knowledge of the ’831 Patent constitutes willful infringement.

FOURTH CAUSE OF ACTION
(INFRINGEMENT OF THE ’897 PATENT)

142. Plaintiff incorporates and realleges all of the above paragraphs as though fully set forth herein.

143. Defendants are not licensed (expressly or impliedly) or otherwise authorized to make, use, offer for sale, or sell any products or services that embody the inventions of the ’897 Patent.

144. Defendants have infringed and continue to infringe, either literally and/or under the doctrine of equivalents, one or more claims of the ’897 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features of the Falcon Platform, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the ’897 Patent.

145. Claim 1 of the ’897 Patent recites:

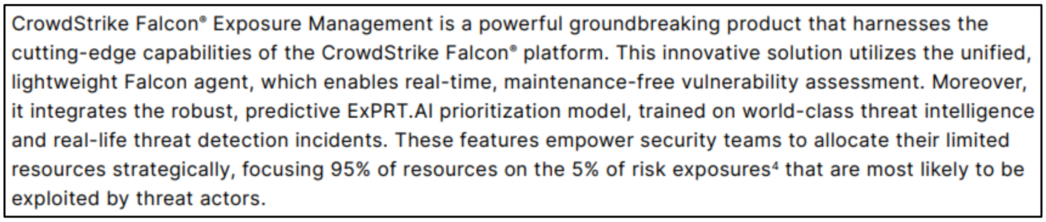
> A method for assessing a likelihood of exploitation of software vulnerabilities, comprising:
>
> utilizing a processor in operable communication with at least one memory for storing instructions that are executed by the processor to perform operations, including:

> accessing a plurality of datasets associated with a predetermined set of data sources, the plurality of datasets including training data comprising hacker communications;
>
> accessing features from the plurality of datasets that include measures computed from social connections of users posting hacking-related content
>
> applying learning algorithms to the training data to generate classification models that are configured to predict class labels defining a likelihood of exploitation of respective software vulnerabilities;
>
> accessing one or more features associated with a software vulnerability; and
>
> computing, by applying the one or more features to the classification model, a class label defining one or more values defining a likelihood of exploitation associated with the software vulnerability, wherein the likelihood of exploitation predicts an actual exploitation of the respective software vulnerabilities before disclosure based on the hacker communications from the training data.

146. As illustrated in the example below,[92] the Falcon Platform performs each step of the method of claim 1 of the '897 Patent. To the extent that the preamble is limiting, the Falcon Platform performs the claimed "*method for assessing a likelihood of exploitation of software vulnerabilities*." For instance, the Falcon Platform is a cloud-based SaaS, which is made up of numerous modules that provide antivirus and related SaaS services. The Falcon Exposure Management module (and its predecessor Falcon Spotlight) assesses and remediates vulnerabilities in a computer environment (a *method for assessing*). Falcon Exposure Management's "Native Vulnerability Assessment . . . [o]btain[s] rich vulnerability details, exploit information and attacker context through first-party and third-party intelligence feeds." The "Network Vulnerability Assessment" uses ExPRT.AI (the Expert Prediction Rating artificial intelligence model) to focus on critical risks "by analyzing real-world exploitability" and CrowdStrike threat intelligence for "real-time insights into exploit status" (*likelihood of*

[92] The following examples are illustrative only and not intended to limit Plaintiff's right to supplement or modify its allegations regarding the exemplary products or to allege that other CrowdStrike products infringe the '897 Patent.

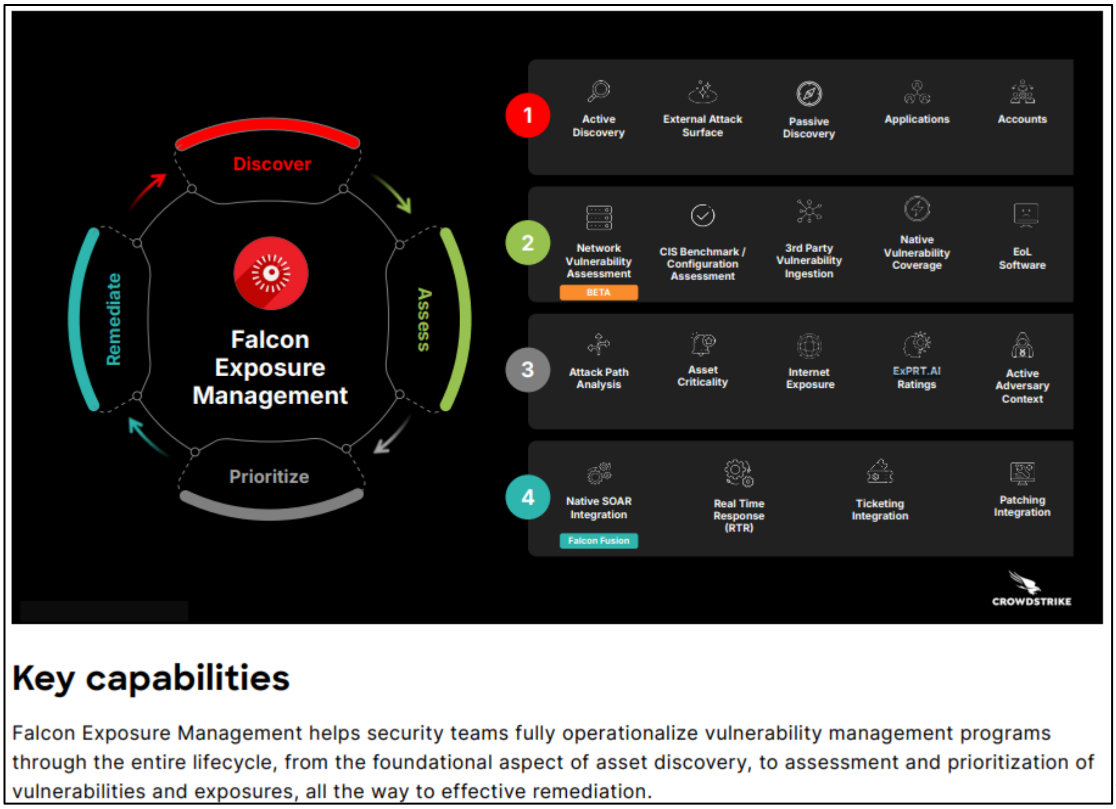
exploitation of software vulnerabilities). Moreover, ExPRT.AI is a "dynamic AI model trained on CrowdStrike's exploit intelligence and real-life detection events" that "narrows down crucial vulnerabilities" and an "Active Adversary Context" "industry-leading threat intelligence" to "pinpoint[] and correlate[] vulnerabilities with adversaries" (and returns a set of vulnerabilities).[93] Furthermore, ExPRT.AI leverages advanced machine learning to enhance accuracy and employs a continuously adapting model to predict the *likelihood of vulnerability exploitation*.[94]



CrowdStrike Falcon® Exposure Management is a powerful groundbreaking product that harnesses the cutting-edge capabilities of the CrowdStrike Falcon® platform. This innovative solution utilizes the unified, lightweight Falcon agent, which enables real-time, maintenance-free vulnerability assessment. Moreover, it integrates the robust, predictive ExPRT.AI prioritization model, trained on world-class threat intelligence and real-life threat detection incidents. These features empower security teams to allocate their limited resources strategically, focusing 95% of resources on the 5% of risk exposures[4] that are most likely to be exploited by threat actors.

[93] https://www.crowdstrike.com/wp-content/uploads/2024/09/falcon-exposure-management-data-sheet.pdf.

[94] https://www.crowdstrike.com/en-us/blog/crowdstrike-falcon-spotlight-fuses-endpoint-data-with-cisa-exploited-vulnerabilities-catalog.



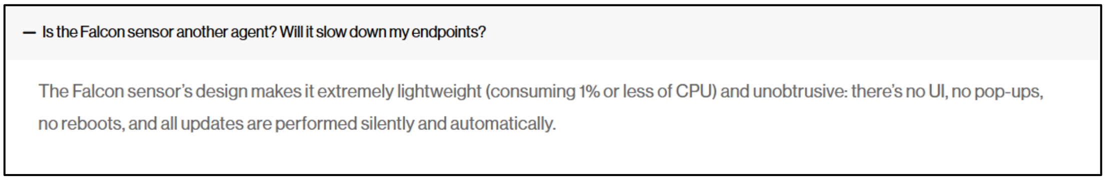
Key capabilities

Falcon Exposure Management helps security teams fully operationalize vulnerability management programs through the entire lifecycle, from the foundational aspect of asset discovery, to assessment and prioritization of vulnerabilities and exposures, all the way to effective remediation.[95]

147. The Falcon Platform performs a method that includes "*utilizing a processor in operable communication with at least one memory for storing instructions that are executed by the processor to perform operations*." For instance, the Falcon Platform's lightweight Falcon sensor "consum[es] 1% or less of CPU [central processing unit]" power (e.g., *utilizing a processor*). Moreover, Falcon Exposure Management uses the Falcon agent/Falcon sensor for vulnerability assessment. As an example, the Falcon sensor utilizes the "CPU to perform accelerated memory scanning for malicious patterns." This process enables "direct communication between the processor and memory to store, retrieve, and analyze extensive memory data, allowing for efficient

[95] https://www.crowdstrike.com/wp-content/uploads/2024/09/falcon-exposure-management-data-sheet.pdf

detection of fileless threats" (e.g., *utilizing a processor in operable communication with at least one memory for storing instructions that are executed by the processor to perform operations*).[96]

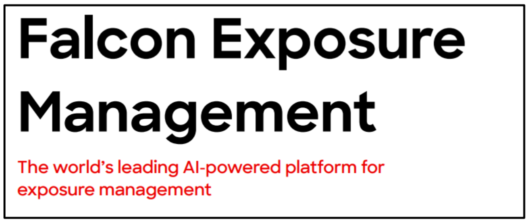


— Is the Falcon sensor another agent? Will it slow down my endpoints?

The Falcon sensor's design makes it extremely lightweight (consuming 1% or less of CPU) and unobtrusive: there's no UI, no pop-ups, no reboots, and all updates are performed silently and automatically.

[97]

148. The Falcon Platform performs a method that includes "*accessing a plurality of datasets associated with a predetermined set of data sources, the plurality of datasets including training data comprising hacker communications*." For instance, Falcon Exposure Management's "Native Vulnerability Assessment . . . [o]btain[s] rich vulnerability details, exploit information and attacker context through first-party and third-party intelligence feeds" (e.g. *accessing a plurality of datasets associated with a predetermined set of data sources*). The "Network Vulnerability Assessment" uses ExPRT.AI to focus on critical risks "by analyzing real-world exploitability" and CrowdStrike threat intelligence for "real-time insights into exploit status" (e.g., *plurality of datasets*). Moreover, ExPRT.AI is a "dynamic AI model trained on CrowdStrike's exploit intelligence and real-life detection events" that "narrows down crucial vulnerabilities" and an "Active Adversary Context" "industry-leading threat intelligence" to "pinpoint[] and correlate[] vulnerabilities with adversaries" (e.g., *plurality of datasets including training data*).

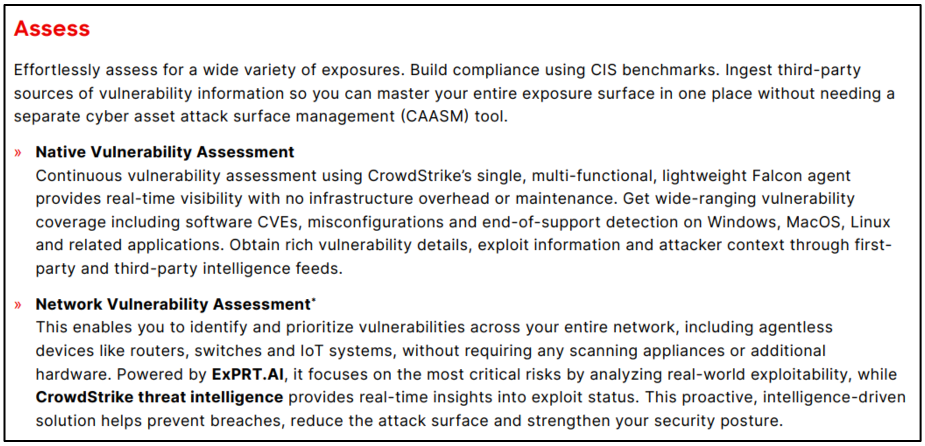


Falcon Exposure Management

The world's leading AI-powered platform for exposure management

[96] https://www.crowdstrike.com/wp-content/uploads/2024/09/falcon-exposure-management-data-sheet.pdf.

[97] https://www.crowdstrike.com/products/faq/

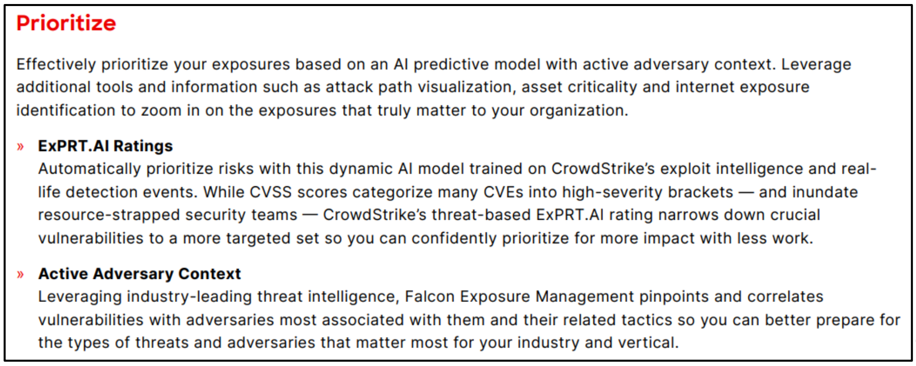


Assess

Effortlessly assess for a wide variety of exposures. Build compliance using CIS benchmarks. Ingest third-party sources of vulnerability information so you can master your entire exposure surface in one place without needing a separate cyber asset attack surface management (CAASM) tool.

» **Native Vulnerability Assessment**
Continuous vulnerability assessment using CrowdStrike's single, multi-functional, lightweight Falcon agent provides real-time visibility with no infrastructure overhead or maintenance. Get wide-ranging vulnerability coverage including software CVEs, misconfigurations and end-of-support detection on Windows, MacOS, Linux and related applications. Obtain rich vulnerability details, exploit information and attacker context through first-party and third-party intelligence feeds.

» **Network Vulnerability Assessment***
This enables you to identify and prioritize vulnerabilities across your entire network, including agentless devices like routers, switches and IoT systems, without requiring any scanning appliances or additional hardware. Powered by **ExPRT.AI**, it focuses on the most critical risks by analyzing real-world exploitability, while **CrowdStrike threat intelligence** provides real-time insights into exploit status. This proactive, intelligence-driven solution helps prevent breaches, reduce the attack surface and strengthen your security posture.



Prioritize

Effectively prioritize your exposures based on an AI predictive model with active adversary context. Leverage additional tools and information such as attack path visualization, asset criticality and internet exposure identification to zoom in on the exposures that truly matter to your organization.

» **ExPRT.AI Ratings**
Automatically prioritize risks with this dynamic AI model trained on CrowdStrike's exploit intelligence and real-life detection events. While CVSS scores categorize many CVEs into high-severity brackets — and inundate resource-strapped security teams — CrowdStrike's threat-based ExPRT.AI rating narrows down crucial vulnerabilities to a more targeted set so you can confidently prioritize for more impact with less work.

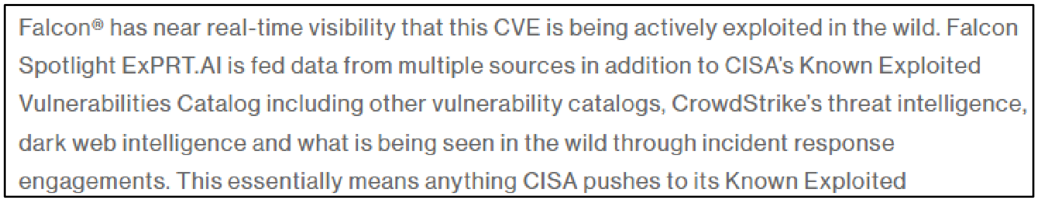
» **Active Adversary Context**
Leveraging industry-leading threat intelligence, Falcon Exposure Management pinpoints and correlates vulnerabilities with adversaries most associated with them and their related tactics so you can better prepare for the types of threats and adversaries that matter most for your industry and vertical.

[98]

149. Indeed, ExPRT.AI processes CrowdStrike data, including EDR, vulnerability management, threat intelligence information, and "dark web intelligence" (e.g., *hacker communications*). Furthermore, CrowdStrike software monitors the dark web to detect data leaks, stolen information, and other hacker-related communications, thereby surveilling hacker activities. This data functions as training data on hacker communications.[99]

[98] https://www.crowdstrike.com/wp-content/uploads/2024/09/falcon-exposure-management-data-sheet.pdf

[99] *See* https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/dark-web-monitoring/.



Falcon® has near real-time visibility that this CVE is being actively exploited in the wild. Falcon Spotlight ExPRT.AI is fed data from multiple sources in addition to CISA's Known Exploited Vulnerabilities Catalog including other vulnerability catalogs, CrowdStrike's threat intelligence, dark web intelligence and what is being seen in the wild through incident response engagements. This essentially means anything CISA pushes to its Known Exploited [100]

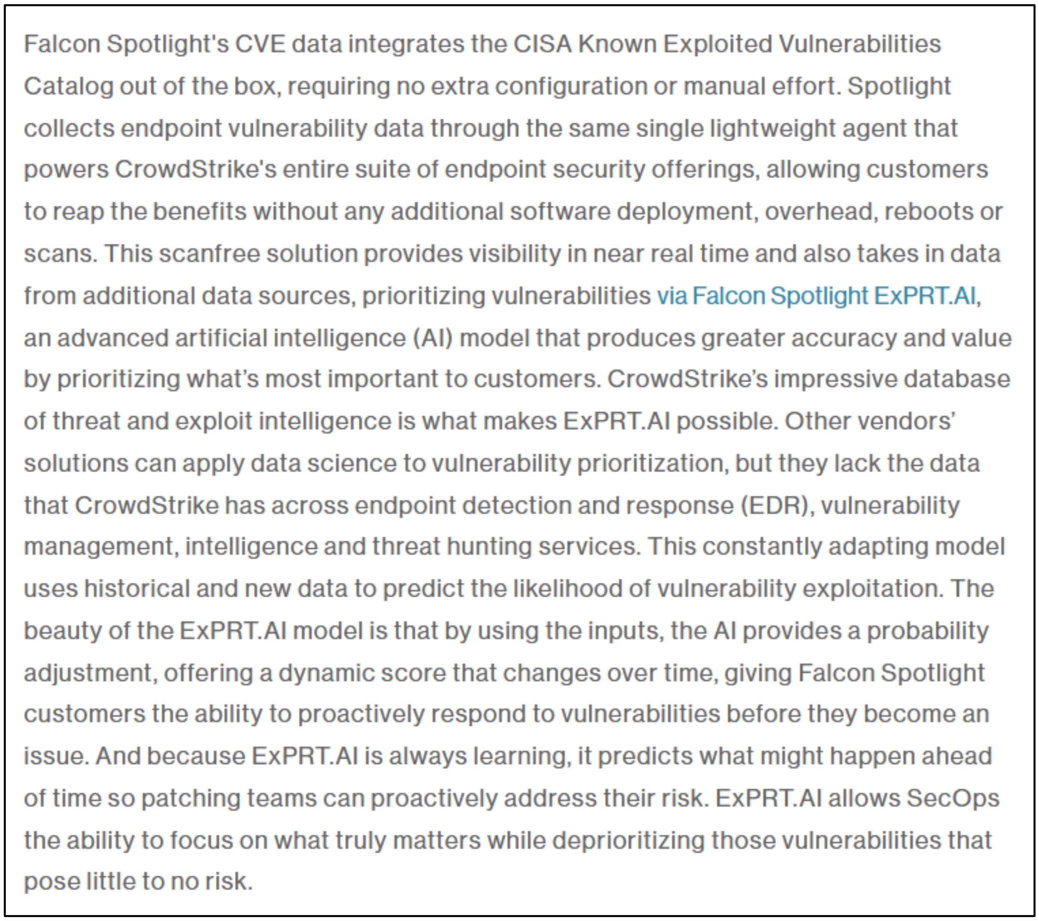
150. The Falcon Platform performs a method that includes "*accessing features from the plurality of datasets that include measures computed from social connections of users posting hacking-related content*." For instance, as previously discussed, CrowdStrike Threat Intelligence modules implement deep and dark web monitoring (accessing features from the plurality of datasets), including "55,000+ unique sites on the deep, dark web" and "500+ million posts to social media" (measures computed from social connections of users posting hacking-related content) in addition to "8+ billion files, posts and messages," and "encrypted messaging apps."[101]

151. The Falcon Platform performs a method that includes "*applying learning algorithms to the training data to generate classification models that are configured to predict class labels defining a likelihood of exploitation of respective software vulnerabilities*." For example, Falcon Spotlight's and Falcon Exposure Management's ExPRT.AI model use historical and new data (e.g., *training data*) on vulnerabilities and threats, applying learning algorithms to continuously enhance its predictive accuracy and refine the model. Developed as a classification model to prioritize vulnerabilities, it assigns each vulnerability a dynamic score or probability, indicating its likelihood of exploitation (e.g., *applying learning algorithms to the training data to generate classification models*). This score functions as a "class label" that adjusts over time,

[100] https://www.crowdstrike.com/en-us/blog/crowdstrike-falcon-spotlight-fuses-endpoint-data-with-cisa-exploited-vulnerabilities-catalog/?srsltid=AfmBOoo31ShUMRmLm7K5xpTE6Y0OI2uSKpNgYrySujSMyf17txAVIxtD

[101] *See* https://www.crowdstrike.com/wp-content/uploads/2022/10/falcon-threat-intelligence-recon-infographic.pdf.

reflecting changing threat levels (e.g., *that are configured to predict class labels defining a likelihood of exploitation of respective software vulnerabilities*).



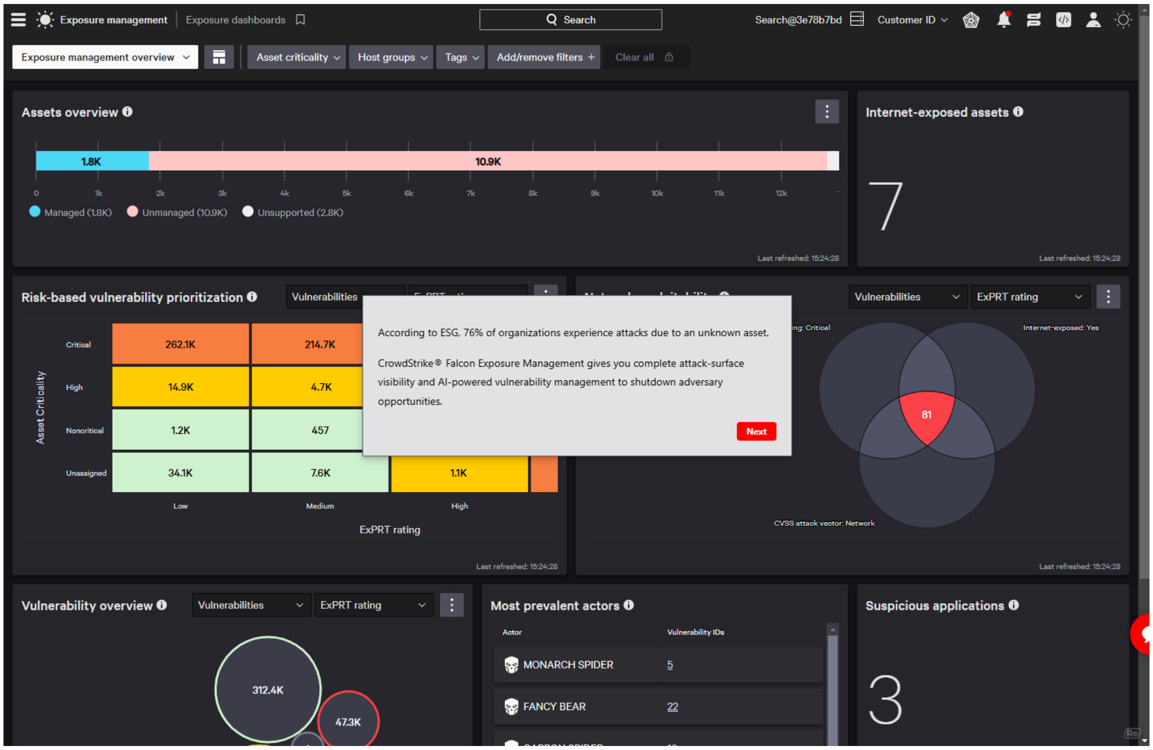
Falcon Spotlight's CVE data integrates the CISA Known Exploited Vulnerabilities Catalog out of the box, requiring no extra configuration or manual effort. Spotlight collects endpoint vulnerability data through the same single lightweight agent that powers CrowdStrike's entire suite of endpoint security offerings, allowing customers to reap the benefits without any additional software deployment, overhead, reboots or scans. This scanfree solution provides visibility in near real time and also takes in data from additional data sources, prioritizing vulnerabilities via Falcon Spotlight ExPRT.AI, an advanced artificial intelligence (AI) model that produces greater accuracy and value by prioritizing what's most important to customers. CrowdStrike's impressive database of threat and exploit intelligence is what makes ExPRT.AI possible. Other vendors' solutions can apply data science to vulnerability prioritization, but they lack the data that CrowdStrike has across endpoint detection and response (EDR), vulnerability management, intelligence and threat hunting services. This constantly adapting model uses historical and new data to predict the likelihood of vulnerability exploitation. The beauty of the ExPRT.AI model is that by using the inputs, the AI provides a probability adjustment, offering a dynamic score that changes over time, giving Falcon Spotlight customers the ability to proactively respond to vulnerabilities before they become an issue. And because ExPRT.AI is always learning, it predicts what might happen ahead of time so patching teams can proactively address their risk. ExPRT.AI allows SecOps the ability to focus on what truly matters while deprioritizing those vulnerabilities that pose little to no risk.

[102]

152. The Falcon Platform performs a method that includes "*accessing one or more features associated with a software vulnerability*." For instance, Falcon Exposure Management implements "AI-powered vulnerability management to shutdown adversary opportunities" (*accessing one or more features associated with a software vulnerability*). As illustrated below, an exemplary Falcon Exposure Management dashboard for a computer environment displays

[102] https://www.crowdstrike.com/en-us/blog/crowdstrike-falcon-spotlight-fuses-endpoint-data-with-cisa-exploited-vulnerabilities-catalog/

vulnerabilities that are rated "Critical" using ExPRT.AI. CrowdStrike software further assess and reports on whether vulnerabilities are "actively used."[103]



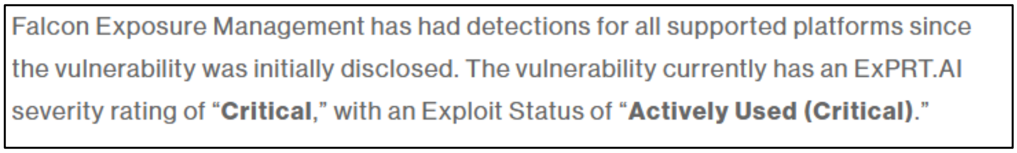
	Low	Medium	High
Critical	262.1K	214.7K	
High	14.9K	4.7K	
Noncritical	1.2K	457	
Unassigned	34.1K	7.6K	1.1K

According to ESG, 76% of organizations experience attacks due to an unknown asset.

CrowdStrike® Falcon Exposure Management gives you complete attack-surface visibility and AI-powered vulnerability management to shutdown adversary opportunities.

Next

Actor	Vulnerability IDs
MONARCH SPIDER	5
FANCY BEAR	22

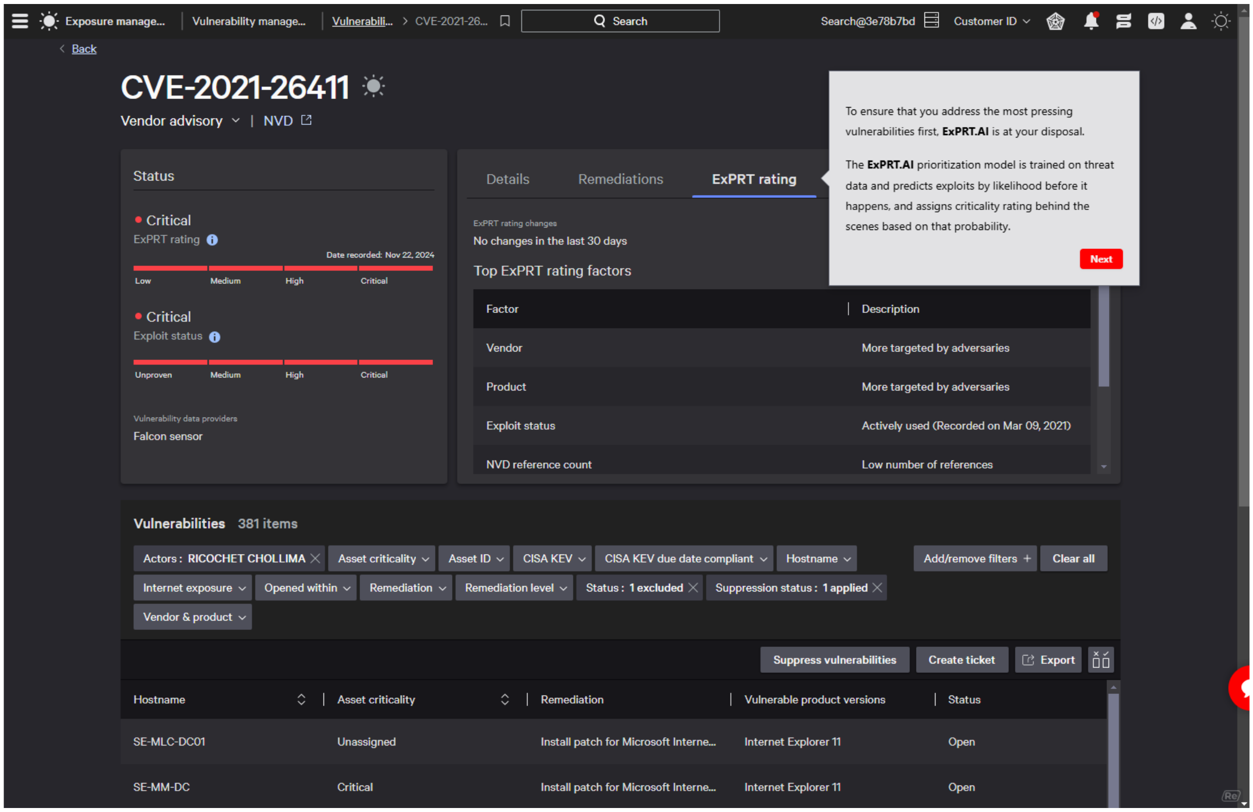


Falcon Exposure Management has had detections for all supported platforms since the vulnerability was initially disclosed. The vulnerability currently has an ExPRT.AI severity rating of "**Critical**," with an Exploit Status of "**Actively Used (Critical)**."[104]

153. The Falcon Platform performs a method that includes "computing, by applying the one or more features to the classification model, a class label defining one or more values defining a likelihood of exploitation associated with the software vulnerability, wherein the likelihood of exploitation predicts an actual exploitation of the respective software vulnerabilities before disclosure based on the hacker communications from the training data." For instance, the Falcon Exposure Management's "ExPRT.AI prioritization model is trained on threat data [(computing, by

[103] *See* https://www.crowdstrike.com/en-us/interactive-demos/falcon-exposure-management/.
[104] https://www.crowdstrike.com/en-us/blog/active-exploitation-linux-kernel-privilege-escalation-vulnerability/

applying the one or more features to the classification model)] and predicts exploits by likelihood before it happens [(defining a likelihood of exploitation associated with the software vulnerability, wherein the likelihood of exploitation predicts an actual exploitation of the respective software vulnerabilities)], and assigns criticality rating [(a class label defining one or more values)] behind the scenes based on that probability" (before disclosure based on the hacker communications from the training data). As shown below, an exemplary vulnerability for "CVE-2021-26411" is displayed on the Falcon Exposure Management dashboard with a "Critical" rating for "ExPRT rating" as well as a "Critical" rating for "Exploit status" (and further noting the "Falcon sensor" as a "Vulnerability data provider").



Exposure manage... | Vulnerability manage... | Vulnerabili... > CVE-2021-26...
Search
Search@3e78b7bd
Customer ID
Back

CVE-2021-26411

Status

● Critical
ExPRT rating
Date recorded: Nov 22, 2024

● Critical
Exploit status

Vulnerability data providers
Falcon sensor

ExPRT rating changes
No changes in the last 30 days

Top ExPRT rating factors

Factor	Description
Vendor	More targeted by adversaries
Product	More targeted by adversaries
Exploit status	Actively used (Recorded on Mar 09, 2021)
NVD reference count	Low number of references

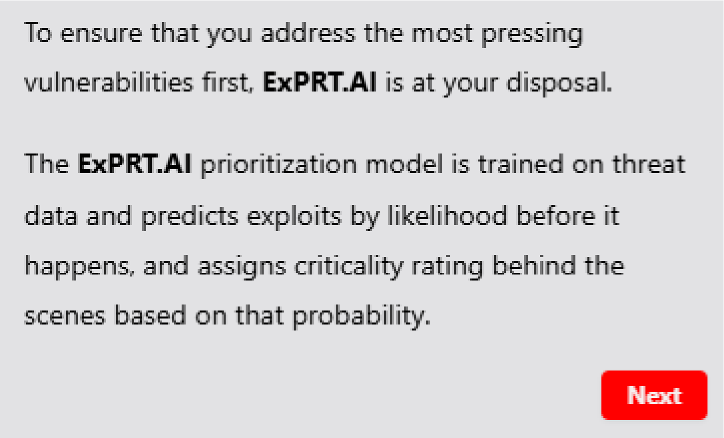
To ensure that you address the most pressing vulnerabilities first, **ExPRT.AI** is at your disposal.

The **ExPRT.AI** prioritization model is trained on threat data and predicts exploits by likelihood before it happens, and assigns criticality rating behind the scenes based on that probability.

Vulnerabilities 381 items

Actors : RICOCHET CHOLLIMA
Status : 1 excluded
Suppression status : 1 applied

Hostname	Asset criticality	Remediation	Vulnerable product versions	Status
SE-MLC-DC01	Unassigned	Install patch for Microsoft Interne...	Internet Explorer 11	Open
SE-MM-DC	Critical	Install patch for Microsoft Interne...	Internet Explorer 11	Open



To ensure that you address the most pressing vulnerabilities first, **ExPRT.AI** is at your disposal.

The **ExPRT.AI** prioritization model is trained on threat data and predicts exploits by likelihood before it happens, and assigns criticality rating behind the scenes based on that probability.

[105]

154. The Falcon Exposure Management's ExPRT.AI model applies "features from multiple data sources," including dark web monitoring, to a classification model. CrowdStrike ExPRT.AI leverages historical and real-time data to evaluate vulnerability features, prioritizing them based on risk level. The model computes and analyzes these features to aid in effective vulnerability prioritization. ExPRT.AI assigns a "dynamic score" as a class label, "indicating the likelihood of exploitation," which adjusts over time to reflect changing threat levels and guides response actions. Meanwhile, dark web monitoring gathers data on "hacker communications and activities," providing early indicators of potential exploitation attempts before vulnerabilities become widely known.[106]

155. Defendants have been aware of the '897 Patent since at least the filing of this Complaint.

156. Defendants' partners, customers, and end users of the Accused Products and corresponding systems and services directly infringe at least claim 1 of the '897 Patent, literally or

[105] https://www.crowdstrike.com/en-us/interactive-demos/falcon-exposure-management/

[106] *See* https://www.crowdstrike.com/en-us/interactive-demos/falcon-exposure-management/; https://www.crowdstrike.com/en-us/blog/crowdstrike-falcon-spotlight-fuses-endpoint-data-with-cisa-exploited-vulnerabilities-catalog/; https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/dark-web-monitoring/.

under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services.

157. Defendants have actively induced and are actively inducing infringement of at least claim 1 of the ’897 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that their acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendants encourage and induce customers to use CrowdStrike’s security software in a manner that infringes claim 1 of the ’897 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products.

158. Defendants encourage, instruct, direct, and/or require third parties—including their certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways.

159. Defendants further encourage and induce their customers to infringe at least claim 1 of the ’897 Patent: 1) by making their security services available on their website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including their CrowdStrike security software, and services in the United States.[107]

160. For example, on information and belief, Defendants share instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above,

[107] https://www.crowdstrike.com/en-us/; https://www.crowdstrike.com/en-us/partners/partner-program/.

including at least customers and partners.[108] On further information and belief, Defendants also provide customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner.[109]

161. Defendants and/or Defendants' partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendants and/or one of Defendants' partners, which obligates each customer to perform certain actions in order to use the Accused Products.[110] Further, in order to receive the benefit of Defendants' and/or their partners' continued technical support and their specialized knowledge and guidance of the operability of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '897 Patent.[111]

162. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendants and/or Defendants' partners affirmatively aid and abet each customer's use of the Accused Products in a manner that performs the claimed method of, and infringes, the '897 Patent.

163. Plaintiff has suffered and continues to suffer damages as a result of Defendants' infringement of the '897 Patent. Defendants are therefore liable to Plaintiff under 35 U.S.C. § 284

[108] https://www.crowdstrike.com/en-us/free-trial-guide/; https://www.crowdstrike.com/en-us/free-trial-guide/start-and-install/.
[109] https://www.crowdstrike.com/contact-us/.
[110] https://www.crowdstrike.com/free-trial-guide/purchase/; https://www.crowdstrike.com/free-trial-guide/installation/).
[111] *See* https://www.crowdstrike.com/contact-us/.

for damages in an amount that adequately compensates Plaintiff for Defendants' infringement, but no less than a reasonable royalty.

164. Plaintiff, its predecessors-in-interest, and/or any licensees have satisfied all statutory obligations required to collect pre-filing damages for the full period allowed by law for infringement of the '897 Patent.

165. On information and belief, despite Defendants' knowledge of the Asserted Patents and Plaintiff's patented technology, Defendants made the deliberate decision to sell products and services that they knew infringe the Asserted Patents. Defendants' continued infringement of the '897 Patent with knowledge of the '897 Patent constitutes willful infringement.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests the following relief:

A. That this Court adjudge and decree that Defendants have been, and are currently, infringing each of the Asserted Patents;

B. That this Court award damages to Plaintiff to compensate it for Defendants' past infringement of the Asserted Patents, through the date of trial in this action, and damages for future infringement of the Asserted Patents, through the expiration dates of the Asserted Patents;

C. That this Court award pre- and post-judgment interest on such damages to Plaintiff;

D. That this Court order an accounting of damages incurred by Plaintiff from six years prior to the date this lawsuit was filed through the entry of a final, non-appealable judgment;

E. That this Court determine that this patent infringement case is exceptional and award Plaintiff its costs and attorneys' fees incurred in this action;

F. That this Court award increased damages under 35 U.S.C. § 284; and

G. That this Court award such other and further relief as the Court deems just and equitable.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff respectfully requests a trial by jury on all issues so triable.

DATED: January 31, 2025

By: */s/ Cecil E. Key*
Cecil E. Key
Jay P. Kesan
KEY KESAN DALLMANN PLLC
1050 Connecticut Avenue, N.W. Suite 500
Washington, DC 20036
Telephone: (202) 772-1100
jay.kesan@kkd-law.com
cecil.key@kkd-law.com

Attorneys for Plaintiff
Skysong Innovations, LLC